**REDRUTH TOWN COUNCIL**

**CONSEL AN DRE RESRUDH**

Redruth Civic Centre, Alma Place, Redruth, Cornwall TR15 2AT
Tel No: 01209-210038 e-mail: admin@redruth-tc.gov.uk

**Town Mayor: Cllr A Biscoe** **Town Clerk: C Williams**

***Our Reference:***
RTC/FC/Nov
***Date:***
25th November 2026

See Distribution

Dear Councillor

## Monthly Meeting of the Redruth Town Council – 30th November 2026

You are summoned to attend a Meeting of the Redruth Town Council to be held in The Langman Room, Redruth Civic Centre, Alma Place on Monday 30th November 2026. Proceedings will commence at 7:00pm.

The Agenda and associated papers are enclosed for your reference and information.

Yours sincerely

Charlotte Williams

Charlotte Williams
Town Clerk
Enclosures

Agenda and associated documentation

Distribution:

Action:

All Redruth Town Councillors

Information:

Press & Public
Cornwall Councillors (Redruth EDs)
Police Inspector

# Redruth Town Council

## Meeting of the Full Council – Monday, 30th November 2026

## AGENDA

PART I - PUBLIC SESSION

1. To receive apologies for absence.

2. Members to declare any disclosable pecuniary interests or non-registerable interests (including details thereof) in respect of any item(s) on this Agenda.

3. Public participation session – to enable the public to put questions to the Council relating to any Town Council matters.

4. To receive reports from the Town Mayor and Deputy Town Mayor.

5. To receive reports from the divisional Cornwall Councillors.

6. To receive correspondence (see attached)

7. To confirm the Minutes of the Monthly Meeting of the Council held on 26th October 2026 (Minutes attached)

8. To receive the Minutes as reports of the following committees and meetings, and to accept and approve the Recommendations and Resolutions contained within the Minutes of the:

   Planning Committee – 26th October 2026 (see attached Minutes)
   Staffing Committee – 16th November 2026 (see attached Minutes)
   Finance Committee – 16th November 2026 (see attached Minutes)
   Annual Town Meeting – 12th November 2026 (see attached Minutes)

9. To consider and approve the following new policies:

   Suite of Data Protection Policies (circulated in October 2026 papers online)

10. To consider the Town Clerk's report. (reports attached)

11. To receive brief verbal updates from Members as representatives on outside bodies.

12. To receive a brief verbal update on the Youth Council.

13. To consider and approve the schedule of payments. (see attached schedule)

PART 11 – PRIVATE SESSION – Exclusion of the Press and Public

The Council is invited to pass the following resolution:- That pursuant to the provisions of the Public Bodies (Admissions to Meetings) Act 1960, the press and public be excluded from the Meeting for the following item of business, by reason of the confidential nature of the business to be transacted.

14. To consider a report from the Deputy Town Clerk and Town Clerk on the Clocktower.

15. To consider essential roof repairs in Market Hall.

**REDRUTH TOWN COUNCIL**

**REPORT FOR: Meeting of Full Council on Monday 30th November 2026**

**SUBJECT OF REPORT: Deputy Mayor's Report**

## SUMMARY OF IMPLICATIONS

| | | |
|---|---|---|
| a. | Policy | No |
| b. | Financial | No |
| c. | Legal | No |

## 1.0 TERMS OF REFERENCE

To report on progress during the period.

## 2.0 REPORT

I organised our community firework display at St Rumons Club, which was very successful indeed, raising over £2400 to be shared between Georgia's voice and Bethel Community Larder.

I also Chaired our annual town meeting at Kressen Kernow, which was very well attended and received by the public. Special thanks to our Officers & Staff for all their efforts in organising this evening.

It was great to see our new ASB officer in attendance, I feel this will be a great asset for our town. I am hoping to attend the ASB drop-in session on 24/11 at the civic centre.

I attended the remembrance parade at Victoria park, followed by a service at St Andrew's Church. Thank you to all who came to show their respect.

I have been liaising with Connor Donithorne to look into a noise complaint from a local resident on Cardrew.

And I am also disappointed that two 'no dogs signs' have been removed from Treskerby play park and I will be reporting this to environment services.

Looking forward to our town light switch on next Saturday.

## 3.0 RECOMMENDATION

That this report is noted.

REDRUTH TOWN COUNCIL

REPORT FOR: Meeting of the Council 30th November

1.0 SUBJECT OF REPORT: Report from C. Cllr Sally Harrison

2.0 SUMMARY OF IMPLICATIONS

| | | | |
|---|---|---|---|
| a. | Policy | - | No |
| b. | Financial | - | No |
| c. | Legal | - | No |

During the past month I have continued to support residents across Redruth South on a range of casework matters, while also attending council, planning and community meetings.

This has been a busy month with casework including vegetation nuisance affecting Clinton Close and Albany Road. This was brought to my attention by Cllr Ian Thomas. Following concerns from residents that overgrown ivy and vegetation were restricting access along the lane, I worked with Cornwall Highways to identify the responsible properties and progress enforcement action. Informal notices were served, and I was pleased to receive confirmation this month that the required hedge-cutting works had now been completed, resolving the issue for residents.

I have also been assisting residents regarding environmental concerns at Jubilee Drive relating to the use of glyphosate spraying on communal areas. I have sought clarification from relevant services, provided updates to residents and continued discussions regarding policy compliance, safe working practices and future management arrangements.

At Cornwall Council level, I attended the Full Council – Extraordinary Meeting and continued to monitor planning and community matters affecting Redruth and the wider area.

Events:- It was an honour to participate and lay a wreath in Redruth's Remembrance Day Parade, joining fellow councillors and residents in commemorating the service and sacrifice of members of the Armed Forces.

Community Chest :-I was pleased to support Trewirgie Infants School with a £100 contribution from my Community Chest towards the replacement of the battery for the school's defibrillator. The device had become unavailable due to the battery reaching the end of its life, and this funding will help ensure the defibrillator is returned to operational use as quickly as possible.

I remain available to residents and local organisations and will continue to progress ongoing casework while representing the interests of Redruth South at both Town and Cornwall Council level.

Cllr.Sally.Harrison@Cornwall.gov.uk

Dear Local Councils,

Many member councils will recall the Public Realm 2027 Working Group convened by CALC and Cornwall Council in August. The group brought together Cornwall Council officers and representatives from town and parish councils to discuss future arrangements for weed management and wider public realm services from 2027 onwards. The discussions identified a potential Service Level Agreement (SLA) model based on local choice, improved mapping information and a funding contribution linked to levels of weed treatment coverage.

Following further consideration of these proposals, CALC sought clarification from Cornwall Council regarding the current position. Earlier this week, the Working Group met with Cornwall Council officers to discuss progress and the implications for the arrangements previously discussed.

**2027/28 Financial Year**
Cornwall Council is continuing to develop its Integrated Weed Management Strategy, which will inform the future approach to weed treatment and public realm management.

An important consideration is the ongoing national review of glyphosate use, with a decision expected in December 2026. The outcome will need to be considered as part of the Council's developing approach to weed management.

Alongside this, the Council is reviewing its programmes and spending commitments as part of its wider budget-setting process. This includes consideration of future public realm arrangements and the resources available to support them.

*Statement from Loic Rich, Cornwall Council's Cabinet Member for Environment and Climate Change:*

*"We recognise the work that town and parish councils have put into developing these proposals and the importance of providing clarity ahead of their precept-setting decisions. However, with the national position on glyphosate still to be confirmed, our*

*Integrated Weed Management Strategy continuing to develop and wider spending commitments under review, we are not in a position to finalise the proposed arrangements for 2027/28. We remain committed to working with local councils to develop opportunities for future partnership working."*

Cornwall Council recognises that this update comes at a difficult point in the precept-setting cycle, with many town and parish councils already preparing their budgets for 2027/28.

Unfortunately, the combination of these outstanding matters means that the proposed arrangements cannot be confirmed in time to provide the certainty councils need when setting their budgets.

As a result, the SLA model discussed by the Working Group will not be introduced for 2027/28.

**Future SLAs**

Cornwall Council remains supportive of the principles discussed by the Working Group, including greater local flexibility, clearer responsibilities and opportunities for partnership working with town and parish councils.

Work is continuing to improve the mapping information needed to support future arrangements, alongside the development of the Integrated Weed Management Strategy.

Although the proposed SLA arrangements cannot be introduced for 2027/28, we'd like to thank them for the work undertaken to date and this has not been lost. It will help inform future options once the national position on glyphosate is confirmed, the Council's approach to weed management has been finalised and there is greater clarity on the resources available to support partnership arrangements.

**Immediate steps**

Any council wishing to undertake additional weed management or public realm activity should therefore plan on the basis of its own priorities and resources.

Further information on future arrangements will be provided as the Integrated Weed Management Strategy and wider budget-setting process progress.

We recognise that this update will be disappointing for councils that have invested time in the Working Group and were considering the proposed arrangements as part of their planning for 2027/28. We also appreciate that the timing presents difficulties for councils already working through their budget-setting process.

While the proposed arrangements cannot progress for 2027/28, the commitment to future partnership working remains, and the work undertaken through the Working Group provides a useful foundation for developing future options.

CALC will continue to work with Cornwall Council on behalf of the sector and will keep member councils informed of significant developments.

Outlook

## RE: Support for Humanities and Social Sciences at the University of Exeter's Penryn Campus

[redacted]

**Date** Tue 27/10/2026 10:06

**To** [redacted]

Dear [redacted]

Thank you for taking the time to share emails from Camborne Town Council and Millbrook Parish Council, expressing their support for Redruth Town Council and their concerns about the proposals on which the University of Exeter consulted. We appreciate the interest shown in our colleagues and the University's work in Cornwall. We responded directly to Redruth Town Council in August, during the consultation period.

Although the letters from Camborne and Millbrook reached us this month, after the formal consultation period had ended, we are grateful that both councils shared their views and wanted to provide a brief update. We would be very happy to contact Camborne and Millbrook directly, or alternatively you may wish to share this response with them – do let us know your preference.

Following a seven-week consultation with affected colleagues and our campus trade unions over the summer, we have now concluded our consideration of the proposed changes in the areas under review. The feedback we received was valuable in helping us to test assumptions, identify risks, consider alternatives and refine a number of the original proposals.

We are pleased to have confirmed that most of the required savings will be achieved through voluntary measures, including the targeted voluntary severance scheme (TERS), planned retirements and reductions in working hours.  Importantly, we have been able to reassure colleagues that compulsory redundancies are no longer being considered as part of this process, either in Cornwall or elsewhere across the University.

We recognise that this has been a difficult and unsettling period for many colleagues and for our wider University community, and we are sincerely grateful to everyone who engaged so thoughtfully and constructively with the consultation. The changes agreed will help us respond to the significant challenges facing the higher education sector while continuing to support our colleagues and plan carefully for the future.

As we emphasised in our earlier correspondence with Redruth Town Council, we remain deeply committed to our campuses in Cornwall and to the University's continuing role in the region. Staffing changes at Penryn have been proportionate to those made across the wider University. We also want to reassure you that the Institute of Cornish Studies is, and will remain, an integral part of Exeter's work in Cornwall.

Thank you again for your engagement.

With best wishes,
Martin

[redacted]
Vice President and Deputy Vice Chancellor (Cornwall)

[redacted]

**Redruth Town Council**

**Consel An Dre Resrudh**

**Redruth Civic Centre, Alma Place, Redruth, Cornwall TR15 2AT**

Tel No: 01209-210038 e-mail: admin@redruth-tc.gov.uk

**Town Mayor: Cllr A Biscoe** **Town Clerk: Mrs C Williams**

# Minutes of a Meeting of the Redruth Town Council held at Redruth Civic Centre, Alma Place, Redruth on Monday 26th October 2026

## Present:

| | |
|---|---|
| Cllr P Broad | Chair |
| Cllr B Ellenbroek | Vice-Chair |
| Cllr E Allen | |
| Cllr S Barnes | |
| Cllr H Biscoe | |
| Cllr K Cunningham | |
| Cllr R Jolly | |
| Cllr D Reeve | |
| Cllr I Thomas | |
| Cllr W Tremayne | |
| Cllr M Selwood | |

## In attendance:

| | |
|---|---|
| Mrs C Williams | Town Clerk |
| Mrs H Bardle | Deputy Town Clerk & Responsible Finance Officer |
| Mrs S Brown | Minute Taker |
| Ms J Turner | Senior Library Officer |
| Mrs J Cockerham-Harris | Administrator |
| Ms L Akerman | Community Liaison Manager |
| Mr T Brown | Communications Manager |

Two members of the public were also in attendance.

DRAFT

## PART I – PUBLIC SESSION

Cllr Broad read the two statements from Redruth Town Council regarding respectful conduct and audio recording of the meeting for minute taking purposes. Redruth Town Council and Cllr Allen declared they were audio recording the meeting.

**1681.1 To receive apologies for absence.**

Apologies were received from Cllr A Biscoe, Cllr Mays, Cllr Morrison, Cllr Connor Donnithorne and Cllr Sally Harrison

**1681.2 Members to declare any disclosable pecuniary interests or non-registerable interests (including details thereof) in respect of any item(s) on this Agenda.**

Cllr Tremayne declared an interest in items 10 and 13 on the Agenda.

**1681.3 Public participation session – to enable members of the public to put questions to the Council relating to any items on the agenda.**

1681.3.1 A member of the public addressed the Cllrs regarding the road resurfacing at the bottom of the High Street causing flooding concerns. The Town Clerk confirmed Cornwall Council Highways are aware of the situation. Cllr Broad noted the comments and asked the Town Clerk to escalate this issue with Cornwall Council again.

1681.3.2 A member of the public advised the Council that the organisation, Fluxus, will be opening in Redruth on Thursday 29th October. They also wanted to raise their concerns regarding the wording of the Social Media Policy, and the strategic Plan. Cllr Broad noted their comments.

**1681.4 To receive reports from the Town Mayor and Deputy Town Mayor.**

1681.4.1 Cllr H Biscoe gave a verbal report on behalf of the Mayor, and the Deputy Mayor summarised his report. Both reports were noted.

**1681.5 To receive reports from the Divisional Cornwall Councillors.**

1681.5.1 No reports were received.

DRAFT

**1681.6 To receive correspondence.**

1681.6.1 The Town Clerk read correspondence from the Events Coordinator, reminding Cllrs of the upcoming Remembrance events and parade and asked that if they were planning on attending, they can confirm to the Events Co-Ordinator.

1681.6.2 The Town Clerk advised the Council that Cllr Tarrant and Coastline Housing had written in and that Coastline would like to give a short presentation of the new Shared Ownership Scheme housing at the next meeting of the Planning Committee.

1681.6.2.1 RESOLVED by Majority to invite Coastline Housing to make the presentation [Proposed Cllr Ellenbroek; Seconded Cllr Reeve; Cllrs Allen and Jolly Abstained].

1681.6.3 The Town Clerk summarised the email from Mr B Ingall, which appealed for funding support and informed the Town Council of the local efforts being made. She also updated on the fact the Town Council have a donations station in the library also and the money will be split between the affected independent businesses. Cllr Cunningham raised concerns about the issue, which have been reported to the police. Cllr Ellenbroek mentioned a fundraising event being held by Krowji. The Town Clerk stated she was meeting with the new ASB Officer this week and she will raise this issue with her also.

**1681.7 To confirm the Minutes of the Monthly Meeting of the Council held on 28th September 2026.**

1681.7.1 RESOLVED by Majority to confirm the minutes of the Monthly Meeting of the Council held on 28th September 2026 [Proposed Cllr H Biscoe; Seconded Cllr Barnes; Cllr Cunningham voted against; Cllr Selwood abstained].

**1681.8 To receive the Minutes as reports of the following committees and meetings, and to accept and approve the Recommendations and Resolutions contained within the Minutes of the:**

**1681.8.1 Planning Committee – 28th September 2026**

1681.8.1.1 RESOLVED by Majority to confirm the Minutes of the Planning Committee held on 28th September 2026 [Proposed Cllr H Biscoe; Seconded Cllr Tremayne; Cllrs Cunningham, Selwood, Allen and Jolly abstained].

DRAFT

**1681.8.2 Community Committee – 5th October 2026**

1681.8.2.1 RESOLVED by Majority to confirm the Minutes of the Community Committee held on 5th October 2026 [Proposed Cllr Ellenbroek; Seconded Cllr Barnes; Cllr Cunningham abstained].

**1681.8.3 Full Council – Extraordinary – 16th December 2024**

1681.8.3.1 RESOLVED by Majority to confirm the Minutes of the Extraordinary Full Council meeting held on 16th December 2024 [Proposed Cllr Ellenbroek; Seconded Cllr H Biscoe; Cllrs Allen and Jolly voted against; Cllrs Selwood and Cunningham abstained].

**1681.8.4 Planning Committee – Extraordinary – 20th October 2026.**

1681.8.4.1 RESOLVED by Majority to confirm the Minutes of the Extraordinary Planning Committee held on 20th October 2026 [Proposed Cllr H Biscoe; Seconded Cllr Tremayne; Cllrs Allen, Jolly and Cunningham abstained].

**1681.9 To consider and approve the following new policies:**

**Suite of Data Protection Policies**
**Data Audit 2026/27**
**IT Policy**

1681.9.1 The Town Clerk clarified that the Council would only be approving the Public Data Protection Policy, The Data Audit Policy and the IT Policy, with the remaining policies to be considered at the next Full Council Meeting.

1681.9.2 Cllr Tremayne requested that the Town Clerks name be removed from the Data Protection Policy and replaced with the title Town Clerk.

1681.9.3 Cllr Jolly asked for clarification on the remaining policies in the Data Policy Suite. The Town Clerk clarified, and Cllr Jolly agreed to send in any additional queries before the next meeting.

1681.9.4 RESOLVED by Majority to approve the policies with Cllr Tremaynes suggested change [Proposed Cllr H Biscoe; Seconded Cllr Barnes; Cllrs Cunningham, Allen and Jolly abstained].

**1681.10 To consider and approve the new Strategic Plan 2026-2031.**

1681.10.1 Cllr Allen expressed concerns about the accessibility, the flexibility and specific wording in the Plan. Cllr Ellenbroek asked the Town Clerk if it would be possible

DRAFT

to produce an easy-read version of the document. The Town Clerk agreed to investigate an easy read version.

1681.10.2 Cllr Jolly echoed Cllr Allen's concern and said that previous objections had not been incorporated into the redesign. She also queried why striving for a Gold Award was an objective. The Town Clerk clarified, stating it was included because it was about raising standards, delivery and attracting additional funding.

1681.10.3 Cllr Broad commended the work that had gone into the Strategic Plan, particularly by the Community Liaison Manager, and highlighted the residents survey that informed the Plan. The Community Liaison Manager was given a round of applause for her work on the Plan.

1681.10.4 Cllrs Ellenbroek and Reeve agreed that the Strategic Plan represented a good starting point for the Council focus going forward, Cllr Reeve requested a change to the order of the document to make the objectives more obvious at the beginning.

1681.10.5 Cllr Selwood thanked the team involved with creating the document, and said he felt it was a good Plan.

1681.10.6 Cllr Jolly queried accessible facility arrangements mentioned in the Plan. The Town Clerk confirmed that the commitment to providing Changing Places provision remains a top priority and will be addressed through work at the Asset Management Committee.

1681.10.7 RESOLVED by Majority to approve the new Strategic Plan 2026-2031 with the re-ordering of the Objectives in the layout. [Proposed Cllr H Biscoe; Seconded Cllr Barnes; Cllrs Allen and Jolly voted against, Cllr Cunningham abstained]

**1681.11 To consider the Town Clerk's two reports.**

**1681.11.1 The Town Clerk summarised the first report.**

1681.11.1.1 Cllr Ellenbroek asked for clarification of GI4G scheme and the sharing of equipment. The Town Clerk confirmed she would return to Cornwall Council for further clarification.

1681.11.1.2 Cllrs Thomas and Tremayne also raised queries regarding the play equipment and maintenance of the parks.

1681.11.1.3 The Town Clerk asked the Council if there was specific data they would like to receive from the new ASB Officer, by way of management reporting. Cllr Selwood requested geographical data, and Cllr Thomas requested the Town Clerk invite

the new Officer to a meeting. The Town Clerk confirmed that the Officer will be invited to a future Council meeting.

1681.11.1.4 RESOLVED by Majority to note the report [Proposed Cllr H Biscoe; Seconded Cllr Barnes; Cllr Cunningham abstained].

**1681.11.2 The Town Clerk summarised the second report on the SLCC national Conference.**

1681.11.2.1 Cllr Selwood requested clarification on Martyn's Law. The Town Clerk gave clarification.

1681.11.2.2 Cllr Ellenbroek stated that the Youth Council were keen to be involved in young makers markets.

1681.11.2.3 Cllr Cunningham stated her interest in organising monthly plant-based markets and looked to the council for support. Cllr Broad and the Town Clerk suggested working with the Climate Action Partnership. (CAPR)

1681.11.2.4 Unanimously RESOLVED to note the report [Proposed Cllr H Biscoe; Seconded Cllr Barnes].

**1681.12 To receive brief verbal updates from Members as representatives on outside bodies**

1681.12.1 Cllr Jolly advised that she would bring a full report on the Real Del Monte Twinning Association to the Community Committee meeting and requested this be on the agenda.

1681.12.2 Cllrs Allen and Barnes gave an update on the Redruth Community Association and commented on the success of the Lowender Festival.

**1681.13 To consider and approve the schedule of payments.**

1681.13.1 Cllr Thomas queried the lone worker security plan and extra staffing cost payments, and whether the costs would be spread across the four councils using the CCTV. The DTC/RFO confirmed the payments related to the CCTV system, and that there was provision in the scheme agreement to pay for staff cover.

1681.13.2 Cllr Barnes queried the changemakers payment. The DTC/RTO advised the payments related to festivals.

1681.13.3 Cllr Allen queried the consort regalia payment. The DTC/RTO explained the payment.

DRAFT

1681.13.4 Unanimously RESOLVED to approve the schedule of payments [Proposed Cllr Broad; Seconded Cllr H Biscoe].

## PART II – PRIVATE SESSION

The Council is invited to pass the following resolution: - That pursuant to the provisions of the Public Bodies (Admissions to the Meetings) Act 1960, the press and public be excluded from the Meeting for the following item of business, by reason of the confidential nature of the business to be transacted.

Unanimously RESOLVED to pass the resolution [Proposed Cllr Reeve; Seconded Cllr H Biscoe].

**1681.14 To consider a report from the Deputy Town Clerk and Town Clerk on the Clocktower.**

1681.14.1 The verbal update was received and noted.

**1681.15 To receive a verbal update on the potential Data Breach investigation.**

1681.15.1 The Town Clerk gave a verbal update and thanked Councillors for their participation in the on-going investigation interviews.

**Chair**

DRAFT

**Redruth Town Council**

**Consel An Dre Resrudh**

Redruth Civic Centre, Alma Place, Redruth, Cornwall TR15 2AT
Tel No: 01209-210038 e-mail: admin@redruth-tc.gov.uk

**Town Mayor: Cllr A Biscoe** **Town Clerk: C Williams**

# Minutes of a Meeting of the Planning Committee held at Redruth Civic Centre, Alma Place, Redruth on Monday 26th October 2026

| | | |
|---|---|---|
| Present: | Cllr H Biscoe | Chair |
| | Cllr W Tremayne | Deputy Chair |
| | Cllr S Barnes | |
| | Cllr P Broad | |
| | Cllr M Selwood | |
| In attendance: | Mrs C Williams | Town Clerk |
| | Mrs H Bardle | RFO/Deputy Town Clerk |
| | Mr S Davey | Minute Taker |
| | There was 1 member of the public in attendance | |

**PART I – PUBLIC SESSION**

**1680.1 To receive apologies for absence**

Apologies were received from Cllrs A Biscoe, Morrison and Reeve.

**1680.2 Members to declare any disclosable pecuniary interests or non-registerable interests (including details thereof) in respect of any item(s) on this Agenda**

None were declared.

**1680.3 Public participation session – to allow members of the public to put questions to the Council relating to any matters relating to the Town Council**

The applicant for planning application PA26/05105 attended the meeting to address the concerns raised by Redruth Town Council and their decision not to support the application. He confirmed that amenity space was sufficient and there is plenty of parking for four properties; four spaces at the front and potentially five spaces at the back. Cllr H Biscoe advised the applicant to speak to the Cornwall Council Planning Officer. Cllr S Barnes advised the applicant to speak to the local Cornwall Councillor for support.

**1680.4 To confirm the Minutes of the Meeting of the Planning Committee held on 28th September 2026.**

RESOLVED by MAJORITY that the minutes of the Planning Committee held on 28th September 2026 be accepted as a true and accurate record of proceedings, [Proposed Cllr S Barnes; Seconded Cllr W Tremayne; Cllr M Selwood abstained].

**1680.5 To confirm the Minutes of the Extraordinary Meeting of the Planning Committee held on 20th October 2026.**

Unanimously RESOLVED that the minutes of the Extraordinary Planning Committee held on 20th October 2026 be accepted as a true and accurate record of proceedings, [Proposed Cllr W Tremayne; Seconded Cllr S Barnes].

**1680.6 To consider the planning applications**

The planning applications were dealt with in accordance with the attached Annex A.

**1680.7 Decision Notice Schedule**

The Decision Notice Schedule was noted.

**1680.8 Licensing Applications**

The Licensing Application Schedule was noted.

**Chair**

DRAFT

**REDRUTH TOWN COUNCIL - PLANNING SCHEDULE**
**ANNEX A**

**All references for PA26 unless otherwise stated.**

**Meeting: Monday 26th October 2026**

**LIST 1**
Unanimously RESOLVED that all the Applications on List 1 are supported en-bloc,
[Proposed Cllr S Barnes; Seconded Cllr M Selwood].

| REF NO | CC REF | SITE AND PROPOSAL | WARD | DECISION |
|---|---|---|---|---|
| 1 | 06765 | The Ladder 2 - 4 Clinton Road Redruth Cornwall<br><br>Listed Building Consent for new side door and internal alterations to create 'youth cafe' in basement rooms. | South | Supported |
| 2 | 06810 | 3 Manor Terrace North Street Redruth Cornwall<br><br>Rear single storey in-fill extension | North | Supported |
| 3 | 07008 | 1 Trewirgie Hill Redruth Cornwall TR15 2TB<br><br>Removal of conservatory and construction of rear kitchen extension | South | Supported |

DRAFT

| | | | | |
|---|---|---|---|---|
| 4 | 07163 | 6 Hoskings Row Redruth Cornwall TR15 2SN<br><br>First floor rear extension to existing dwelling with the inclusion of a Juliet balcony on the north-east elevation. | North | Supported |
| 5 | 07159 | 27 Blights Row Redruth Cornwall TR15 1JL<br><br>Non-material amendment in relation to decision notice PA22/00921 dated 08.04.2022 to allow mono-pitch porch roof to be raised in height above that previously approved. Change roofing materials from glass to natural slate | North | Supported |

## LIST 2

| REF NO | CC REF | SITE AND PROPOSAL | WARD | DECISION |
|---|---|---|---|---|
| 6 | 05846 | | Central | Unanimously RESOLVED to Support the application [Proposed Cllr H Biscoe; Seconded Cllr W Tremayne] |

DRAFT

REDRUTH TOWN COUNCIL

CONSEL AN DRE RESRUDH

**Redruth Civic Centre, Alma Place, Redruth, Cornwall TR15 2AT**
Tel No: 01209-210038 e-mail: admin@redruth-tc.gov.uk

**Town Mayor: Cllr A Biscoe** **Town Clerk: Mrs C Williams**

# Minutes of a Meeting of the Redruth Town Council Staffing Committee held at Redruth Civic Centre, Alma Place, Redruth on Monday 16th November 2026

## Present:

| | |
|---|---|
| Cllr D Reeve | Chair |
| Cllr P Broad | |
| Cllr R S Barnes | |
| Cllr A Biscoe | |
| Cllr H Biscoe | |
| Cllr B Ellenbroek | |
| Cllr A Mays | |
| Cllr M Selwood | |
| Cllr I Thomas | |
| Cllr W Tremayne | |

## In attendance:

| | |
|---|---|
| Cllr J Morrison | |
| Mrs C Williams | Town Clerk |
| Mrs H Bardle | Deputy Town Clerk & Responsible Finance Officer (minute-taker) |

## PART I - PUBLIC SESSION

The Chair read the Welcome Statements.
No recordings of the meeting were disclosed.

**1682.1 To receive apologies for absence**

Apologies were received from Cllrs E Allen and R Jolly, and from Mrs C Rundle, the HR Manager.

**1682.2 Members to declare any disclosable pecuniary interests or non-registerable interests (including details thereof) in respect of any item(s) on this Agenda**

None were declared.

**1682.3 To confirm the Minutes of the Meeting of the Staffing Committee held on 13th July 2026**

**1682.3.1** RESOLVED by MAJORITY to accept the Minutes of the Meeting of the Staffing Committee held on 13th July 2026 as a true and accurate record of proceedings [Proposed Cllr A Biscoe, Seconded Cllr Broad]. Cllrs Ellenbroek, Mays and Tremayne abstained as they had not attended the previous meeting.

Cllr Barnes requested confirmation that he was a member of the Staffing Committee as his name had been excluded from the summons, although he was listed as present at the meeting. The Town Clerk confirmed that he is a member of the Staffing Committee and undertook to ensure the summons is corrected for future meetings.

**1682.4 To exclude the press and public from the meeting for the remaining item of business as their presence would be prejudicial to the public interest by virtue of the confidential nature of the subject matter (employee terms and conditions), and on the grounds that it involves the likely disclosure of exempt information as defined in Part 1 of Schedule 12[A] of the 1972 Local Government Act**

**1682.4.1** Unanimously RESOLVED to exclude the press and public from the meeting for the remaining item of business as their presence would be prejudicial to the public interest by virtue of the confidential nature of the subject matter (employee terms and conditions), and on the grounds that it involves the likely disclosure of exempt

information as defined in Part 1 of Schedule 12[A] of the 1972 Local Government Act. [Proposed Cllr Barnes; Seconded Cllr A Biscoe].

## PART II – PRIVATE SESSION

**1682.5 To consider the report of the HR Manager**

**1682.5.1** The report had been circulated prior to the meeting. The Chair asked for confirmation that no-one was recording this section of the meeting. Unanimously RESOLVED to accept the report. [Proposed Cllr S Barnes; Seconded Cllr A Biscoe]

**Chair**

**Redruth Town Council**

**Consel An Dre Resrudh**

**Redruth Civic Centre, Alma Place, Redruth, Cornwall TR15 2AT**

Tel No: 01209-210038 e-mail: admin@redruth-tc.gov.uk

**Town Mayor: Cllr A Biscoe** **Town Clerk: Mrs C Williams**

# Minutes of a Meeting of the Finance Committee held at Redruth Civic Centre, Alma Place, Redruth on Monday 16th November 2026

## Present:

| | |
|---|---|
| Cllr S Barnes | Chair |
| Cllr H Biscoe | Vice-Chair |
| Cllr D Reeve | |
| Cllr A Mays | |
| Cllr W Tremayne | |
| Cllr E Allen | |
| Cllr R Jolly | |
| Cllr I Thomas | |
| Cllr A Biscoe | |
| Cllr P Broad | |
| Cllr M Selwood | |

## In attendance:

| | |
|---|---|
| Mrs C Williams | Town Clerk |
| Mrs H Bardle | Deputy Town Clerk & Responsible Finance Officer |
| Mrs S Brown | Minute Taker |
| Mrs J Turner | Senior Library Officer |
| Mrs J Pelham-Wales | Business Liaison Manager |
| Ms L Akerman | Community Liaison Manager |
| Mr S Davey | Finance Assistant |
| Mr T Brown | Communications Manager |
| Cllr J Morrison | |

28 Members of the public were also in attendance.

DRAFT

## PART I – PUBLIC SESSION

Cllr Barnes read the two statements from Redruth Town Council regarding respectful conduct and audio recording of the meeting for minute taking purposes. Cllr Allen declared she was audio recording the meeting, and Redruth Town Council declared they were recording the meeting for the purpose of supporting minute preparation only.

**1683.1 To receive apologies for absence**

1683.1.1 No apologies were received.

**1683.2 Members to declare any disclosable pecuniary interests or non-registerable interests (including details thereof) in respect of any item(s) on this Agenda**

1683.2.1 Cllrs Barnes, Reeve, Tremayne, Jolly, and Allen all declared an interest in item 11 on the Agenda, and the register was signed accordingly.

1683.2.2 The Town Clerk informed the meeting that Officers are not required to declare an interest in the same way that Members are, but on this occasion, she has volunteered to do so for transparency purposes. She declared that she is a volunteer, unpaid director of Youth Cafes Cornwall Community Interest Company, who have not applied for funds, but because Young People Cornwall' grant application mentions Hideaway 77 youth café, she wanted to make the declaration.

**1683.3 Public participation session – to enable members of the public to put questions to the Council relating to any items on the agenda**

1683.3.1 A member of the public spoke in support of the grant application for the Hub, Skills over Schools, and drew attention to the services the Hub provides to the community.

1683.3.2 Three members of the public addressed the council to support the grant application from Young People Cornwall, highlighting the positive impact they feel the organisation has on young people and the local community.

1683.3.3 A member of the public declared their support for the grant application submitted by Duchy CIC, speaking about the benefits and positive impact of the programmes they offer to the community.

DRAFT

1683.3.4 A member of the public addressed councillors supporting the application made by Fluxus, drawing attention to the benefits of the organisation to the community, stating a grant would help to fund their work with young people.

1683.3.5 A member of the public spoke to support the grant application from Giant Arts, explaining the benefits to the community.

1683.3.6 A member of the public spoke in support of the application made by the Redruth Football Club highlighting the benefits of the work they do.

1683.3.7 A member of the public spoke in support of Duchy Diamonds highlighting the positive impact of the majorettes group, and how funding would pay for the hire of the school hall which would benefit the wider community.

**1683.4 To confirm the Minutes of the Meeting of the Finance Committee held on 13th July 2026**

Cllr Thomas pointed out that the agenda referred to the wrong date and it was agreed it would be amended.

1683.4.1 Unanimously RESOLVED to confirm the Minutes of the Meeting of the Finance Committee held on 13th July 2026 [Proposed by Cllr Barnes; Seconded by Cllr Mays]

**1683.5 To receive the report from the Business Liaison Manager for the period to 31st October 2026**

1683.5.1 Cllr Allen queried if there had been an increase in sign-ups for UK-PAC, and the Business Liaison Manager confirmed that the process had been made easier for businesses to join, and sign-ups had increased.

1683.5.2 Cllr Barnes commended the Business Liaison Manager for her hard work and efforts, to which everyone agreed.

1683.5.3 Unanimously RESOLVED to note the report [Proposed by Cllr Barnes; Seconded by Cllr A Biscoe]

**1683.6 To review the Management Report for the seven months to 31st October 2026**

1683.6.1 Cllr Allen queried when the council would next have the opportunity to review the management figures for each committee, and Cllr Selwood queried what some of

the costs related to. The DTC/RFO advised that the committee budget reports would be made available soon and clarified the costs for Cllr Selwood.

1683.6.2 Unanimously RESOLVED to note the report [Proposed by Cllr Barnes; Seconded by Cllr H Biscoe]

**1683.7 To approve the assessment of Financial Risks for 2026/27**

1683.7.1 The DTC/RFO confirmed that she will report on the action points at the next meeting of the Finance Committee. Cllr Allen queried whether quarterly monitoring would help track progress better.

1683.8.2 Cllr Thomas queried the frequency of DBS checks for staff and volunteers. The DTC/RFO responded that DBS checks are carried out every three years.

1683.8.3 RESOLVED by majority to approve the report [Proposed by Cllr Barnes; Seconded by Cllr A Biscoe, Cllr Jolly abstained].

**1683.8 To confirm the internal controls for 2025/26 and 2026/27 to date**

1683.8.1 Cllr Allen queried the risk management software used and requested an amendment to the wording for clarity; she also queried the section regarding financial reports prior to meetings. The DTC/RFO advised that the risk management software used for Assets is Civic.ly, but that other risk management is carried out manually on spreadsheets and confirmed that the wording would be changed. The DTC/RFO also advised that up-to-date management accounts will be provided prior to each committee meeting, going forward.

1683.8.2 The report was noted, and the DTC/RFO confirmed she will bring back an amended report for the January Finance meeting.

**1683.9 To receive the internal audit report for Q1 2026/27**

1683.9.1 The DTC/ RFO advised that she would email the two councillors selected, with dates to complete their quarter 2 audit.

1683.9.2 Unanimously RESOLVED to note the report [Proposed by Cllr Barnes; Seconded by Cllr H Biscoe].

DRAFT

**1683.10 To receive a 2027/28 Budget progress report from the DTC/RFO and consider a suggested timetable for approval**

1683.10.1 The DTC/RFO advised that at the time of publishing the papers, the tax base had not been received.

1683.10.2 Cllr Tremayne queried why the Planning Committee wasn't included in the timetable for the budget. The DTC/RFO advised that the Planning Committee was not included because it does not have a budget.

Due to Members disclosable pecuniary interests or non-registerable interests, Cllrs Barnes, Reeve, Tremayne, Jolly and Allen left the meeting. The Town Clerk also left the meeting.

Cllr H Biscoe took the Chair.

**1683.11 To consider the grant applications received for the period to 31st August 2026**

1683.11.1 The DTC/RFO presented a summary of the grant applications to the Council and made the recommendation to carry forward an amount of the available grant funds for the next quarter.

1683.11.2 Cllr Broad suggested that the council prioritise grants from organisations that are located within Redruth, to which Cllr Thomas agreed. Cllr Morrison stated that he felt that no funds should be held back during this round of applications, and each application should be assessed on their own merit. The DTC/RFO clarified that grant funding rounds were due to be held quarterly, but that the next round in January would not be possible if all funds were awarded during this meeting. The next round of available funding would then be July 2027.

1683.11.3 It was proposed by the council to not consider grants from organisations that have their main location outside of Redruth. This included grant applications from Portreath Pilot Gig Club, Penlee Family Project, and the RAF Air Cadets (ATC) – 77 Squadron – Redruth.

1683.11.3.1 Unanimously RESOLVED not to make awards to grant applicants located outside of Redruth [Proposed by Cllr H Biscoe; Seconded by Cllr Mays]

1683.11.4 It was also proposed not to make awards to Redruth Community Association, and the Redruth and District Chamber of Commerce, as the Town Council is

providing financial support to the Community Centre and Town Markets in other ways.

1683.11.4.1 Unanimously RESOLVED not to make awards to Redruth Community Association and Redruth and District Chamber of Commerce [Proposed by Cllr Thomas; Seconded by Cllr Selwood]

1683.11.5 It was then proposed to judge the rest of the applications on their own merit and not to intentionally hold back any funds for future rounds.

1683.11.5.1. Unanimously RESOLVED not to intentionally withhold funds for the next round [Proposed by Cllr Selwood; Seconded by Cllr Mays]

1683.11.6 The remaining grants were individually considered and awarded as per the table below.

DRAFT

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **COMMUNITY GRANTS – SMALL GRANTS – up to £500** | | | | |
| 1 | Portreath Pilot Gig Club | £452.80 | NIL | Unanimously RESOLVED not to make awards to grant applicants located outside of Redruth [Proposed by Cllr H Biscoe; Seconded by Cllr Mays] |
| 2 | Penlee Family Project | £500.00 | NIL | Unanimously RESOLVED not to make awards to grant applicants located outside of Redruth [Proposed by Cllr H Biscoe; Seconded by Cllr Mays] |
| 3 | Redruth Tennis Club | £350.00 | £175.00 | Unanimously RESOLVED to award £175.00 [Proposed by Cllr A Biscoe; Seconded by Cllr Mays] |
| 4 | Veterans Regroup CIC | £500.00 | £300.00 | Cllr Mays proposed paying the full grant amount, which was not supported.<br>Unanimously RESOLVED to award £300.00 [Proposed by Cllr Broad; Seconded by Cllr Thomas] |

DRAFT

*Further details from grant applications can be found on the published meeting papers*

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **COMMUNITY GRANTS – SMALL GRANTS – up to £500** | | | | |
| 5 | Circo Kernow | £500.00 | NIL | Cllr Thomas queried the application which states a September start, which would amount to a retrospective award which goes against grant application guidelines<br>Unanimously RESOLVED not to award any money for this grant application.<br>[Proposed by Cllr Thomas; Seconded by Cllr Mays] |
| 6 | Redruth and District Twinning Association | £500.00 | NIL | Unanimously RESOLVED not to make an award [Proposed by Cllr Mays; Seconded by Cllr Selwood] |
| 7 | Crash (Cardiac Rehabilitation & Support) | £500.00 | NIL | RESOLVED by majority not to make an award [Proposed by Cllr Mays; Seconded by Cllr Broad] Cllr Thomas abstained |
| 8 | Redruth Clothes Bank | £360.00 | £180.00 | Cllr A Biscoe proposed a payment of £300.00, which was not supported.<br>Unanimously RESOLVED to award £180.00 [Proposed by Cllr Mays; Seconded by Cllr Selwood] |

DRAFT

*Further details from grant applications can be found on the published meeting papers*

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **COMMUNITY GRANTS – SMALL GRANTS – up to £500** | | | | |
| 9 | Redruth Community Association | £500.00 | NIL | Unanimously RESOLVED not to make an award [Proposed by Cllr Thomas; Seconded by Cllr Selwood] |
| 10 | Redruth and District Chamber of Commerce | £500.00 | NIL | Unanimously RESOLVED not to make an award [Proposed by Cllr Thomas; Seconded by Cllr Selwood] |
| 11 | Kekezza | £500.00 | £250.00 | Unanimously RESOLVED to award £250.00 [Proposed by Cllr A Biscoe; Seconded by Cllr Thomas] |
| | | | | |
| **TOTAL FUNDS** | | £5,162.80 | **£905** | |

DRAFT

*Further details from grant applications can be found on the published meeting papers*

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **COMMUNITY GRANTS - LARGE GRANTS – up to £2,500** | | | | |
| 1 | Redruth Town Band | £2,500 | £1,000 | Cllr Broad proposed £1,500, seconded by Cllr Thomas.<br><br>Cllr H Biscoe proposed to make an amendment to award £1,000, supported by Cllr Selwood. Unanimously RESOLVED to accept the amendment.<br><br>Unanimously RESOLVED to approve the substantive motion to award £1,000 [Proposed by Cllr H Biscoe; Seconded by Cllr Selwood]. |
| 2 | Make It Better | £2,500 | NIL | Unanimously RESOLVED not to make an award [Proposed by Cllr H Biscoe; Seconded by Cllr Mays] |
| 3 | Hidden Help | £2,500 | £1,000 | Unanimously RESOLVED to make an award of £1,000 [Proposed by Cllr A Biscoe; Seconded by Cllr Broad] |

DRAFT

*Further details from grant applications can be found on the published meeting papers*

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **COMMUNITY GRANTS - LARGE GRANTS – up to £2,500** | | | | |
| 4 | Giant Arts CIC | £2,500 | £625 | Cllr Thomas proposed £625, Cllr Broad proposed to make an amendment to award £1000, supported by Cllr Selwood. RESOLVED by majority not to accept the amendment [Proposed by Cllr Broad; Seconded by Cllr Selwood] Cllrs A Biscoe, H Biscoe, and Thomas against.<br><br>RESOLVED by majority to accept the proposal to award £625 [Proposed by Cllr Thomas; Seconded by Cllr A Biscoe], Cllr Mays voted against. |
| 5 | The Ladder | £2,350 | NIL | RESOLVED by majority not to make an award [Proposed by Cllr H Biscoe; Seconded by Cllr Mays] Cllr Selwood abstained |
| 6 | Redruth United Football Club | £2,500 | £1,500 | Cllr H Biscoe proposed £2,000, seconded by Cllr Mays.<br><br>Cllr Broad proposed to make an amendment to award £1,500, supported by Cllr Thomas. Unanimously RESOLVED to accept the amendment.<br><br>Unanimously RESOLVED to approve the substantive motion to award £1,500 [Proposed by Cllr Broad; Seconded by Cllr Thomas]. |

*Further details from grant applications can be found on the published meeting papers*

DRAFT

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **COMMUNITY GRANTS - LARGE GRANTS – up to £2,500** | | | | |
| 7 | Cornwall Neighbourhoods for Change | £2,500 | £1,000 | RESOLVED by majority to make an award of £1,000 [Proposed by Cllr A Biscoe; Seconded by Cllr Thomas] Cllr H Biscoe against |
| 8 | Georgia's Voice | £2,500 | £1,000 | Unanimously RESOLVED to make an award of £1,000 [Proposed by Cllr Broad; Seconded by Cllr Thomas] |
| 9 | Ignite You CIC | £2,100 | £1,000 | Unanimously RESOLVED to make an award of £1,000 [Proposed by Cllr Selwood; Seconded by Cllr A Biscoe] |
| 10 | Make A Mends | £2,500 | NIL | Unanimously RESOLVED not to make an award [Proposed by Cllr Mays; Seconded by Cllr Broad] |
| 11 | Creative Kernow | £2,500 | £1,250 | RESOLVED by majority to make an award of £1,250 [Proposed by Cllr A Biscoe; Seconded by Cllr Thomas] Cllr Mays abstained |
| 12 | Redruth Memory Café | £2,500 | NIL | Unanimously RESOLVED not to make an award [Proposed by Cllr A Biscoe; Seconded by Cllr Mays] |

DRAFT

*Further details from grant applications can be found on the published meeting papers*

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **COMMUNITY GRANTS - LARGE GRANTS – up to £2,500** | | | | |
| 13 | Grow Box | £2,500 | NIL | Unanimously RESOLVED not to make an award [Proposed by Cllr H Biscoe; Seconded by Cllr Selwood] |
| 14 | Duchy Collective | £2,500 | £1,700 | Unanimously RESOLVED to make an award of £1,700 [Proposed by Cllr Mays; Seconded by Cllr Broad] |
| 15 | Resilient Orchards Cornwall CIC | £1,445 | £772 | Unanimously RESOLVED to make an award of £772 [Proposed by Cllr Mays; Seconded by Cllr A Biscoe] |
| | | | | |
| **TOTAL FUNDS** | | £35,895 | **£10,847** | |

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **YOUTH GRANTS - SMALL GRANTS – up to £500** | | | | |
| 1 | 1st St Andrews Brownies | £500 | £400 | Cllr A Biscoe proposed payment of the full amount. Cllr Thomas proposed an amendment to pay £400.<br>Unanimously RESOLVED to award £400 [Proposed by Cllr Thomas; Seconded by Cllr A Biscoe] |

*Further details from grant applications can be found on the published meeting papers*

DRAFT

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **YOUTH GRANTS - SMALL GRANTS – up to £500** | | | | |
| 2 | Heart Heroes | £250 | £250 | Unanimously RESOLVED to award £250 [Proposed by Cllr Thomas; Seconded by Cllr Selwood] |
| | | | | |
| **TOTAL FUNDS** | | £750 | **£650** | |

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **YOUTH GRANTS - LARGE GRANTS – up to £2,500** | | | | |
| 1 | Carefree Cornwall | £2,400 | £1,000 | RESOLVED by majority to award £1,000 [Proposed by Cllr Thomas; Seconded by Cllr Broad] Cllr Mays voted against |
| 2 | RAF Air Cadets (ATC) – 77 Squadron – Redruth | £2,460 | NIL | Unanimously RESOLVED not to make awards to grant applicants located outside of Redruth [Proposed by Cllr H Biscoe; Seconded by Cllr Mays] |
| 3 | Penhaligons' Friends | £2,500 | £1,000 | Unanimously RESOLVED to award £1,000 [Proposed by Cllr Thomas; Seconded by Cllr Selwood] |
| | | | | |
| **TOTAL FUNDS** | | £7,630 | **£2,000** | |

*Further details from grant applications can be found on the published meeting papers*

DRAFT

| | Applicant | Amount Applied for | Amount Awarded | Decision |
|---|---|---|---|---|
| **YOUTH GRANTS - MAXI GRANTS – up to £20,000** | | | | |
| 1 | Skills Over School Project CIC | £20,000 | £9,500 | It was proposed by Cllr Broad that half of the application amount is paid to each applicant, which totalled more than the remaining award fund. Cllr Selwood proposed 45%. The DTC/RFO confirmed that approximately 47.5% of the requested funds for each applicant would be within the remaining budget amount.<br><br>RESOLVED by majority to award the suggested amounts to each applicant. [Proposed by Cllr Thomas; Seconded by Cllr Broad] Cllr Mays voted against |
| 2 | Gwealan Tops | £19,959 | £9,500 | |
| 3 | Duchy Diamonds | £8,000 | £4,000 | |
| 4 | Young People Cornwall | £19,992 | £9,500 | |
| 5 | Fluxus | £5,000 | £2,500 | |
| | | | | |
| **TOTAL FUNDS** | | £72,951 | **£35,000** | |

**Chair**

DRAFT

*Further details from grant applications can be found on the published meeting papers*

**REDRUTH TOWN COUNCIL** **CONSEL AN DRE RESRUDH**

Redruth Civic Centre, Alma Place, Redruth, Cornwall TR15 2AT
Tel No: 01209-210038 e-mail: admin@redruth-tc.gov.uk

**Town Mayor: Cllr A Biscoe** **Town Clerk: C Williams**

Minutes of The Annual Town Meeting held at Kresen Kernow
on Thursday 12th November 2026

| | | | |
|---|---|---|---|
| Present: | Cllr A Biscoe | Town Mayor | Chair |
| | Cllr P Broad | Deputy Mayor | |
| | Cllr E Allen | | |
| | Cllr S Barnes | | |
| | Cllr H Biscoe | | |
| | Cllr K Cunningham | | |
| | Cllr B Ellenbroek | | |
| | Cllr R Jolly | | |
| | Cllr A Mays | | |
| | Cllr D Reeve | | |
| | Cllr M Selwood | | |
| | Cllr I Thomas | | |
| In attendance: | C Williams | Town Clerk | |
| | H Bardle | Deputy Town Clerk/Responsible Finance Officer | |
| | J Turner | Senior Library Officer | |
| | L Akerman | Community Liaison Manager | |
| | J Pelham-Wales | Business Liaison Manager | |
| | T Brown | Communications Manager | |
| | G Coombs | Facilities Manager | |
| | S Denyer | Deputy Library Manager | |
| | J Cockerham-Harris | Creative Co-ordinator | |
| | S Phillips | Library and Information Assistant | |
| | B Eyriey | Marketing Co-ordinator | |
| | M Mantell | Events Co-ordinator | |
| | M Young | ASB Caseworker | |
| | T Hendy | Website Designer | |

Approximately 80 members of the public were present at the meeting.

DRAFT

The meeting commenced at 6.50pm with a welcome from the Town Mayor, Cllr Alison Biscoe.

The Town Clerk, Charlotte Williams, addressed the meeting:

*Welcome. On behalf of the staff team I'd like to say thank you for being here. We really appreciate your time and it's very important that we listen to you.*
*As our Town Mayor said, we will be holding an Annual Town meeting between 1st March and 1st June 2027, and I am personally sorry that tonight is not in that statutory window. That mistake is mine to own.*
*However, I'd like to share with you some of the staff team priorities in the coming few months. On arrival you were given a summary of the Strategic Plan. In January we'll be publishing how and when we plan to implement the identified actions for People, for Place and for Nature in an Implementation Plan. Some of the actions have already begun. Subjects the team will be working to deliver include, for example,*

- *How and when will Councillor Surgeries start?*
- *How and when will we seek to have a Changing Places toilet in the Town Centre?*
- *How and when can we bring a Community Post Office to town?*

*to name just a few.*
*As we all know, funding nationally and locally is getting harder but this year, Council has increased its grants pot from £16k to £56k to give more to grassroots community organisations like those you are involved in.*
*The team will continue to look for new funding that isn't taxpayers' money. Last year, in grants, we brought in over £400,000 in addition to section 106 money and Community Infrastructure Levy money from local developments, which is being used to purchase play equipment.*
*We've also raised funds as a team by volunteering for three charities; Penhaligon's Friends, Readeasy and MacMillan Cancer Support.*
*I'd also like to acknowledge that we don't always get it right, but we do always listen. For example, we've introduced changes to our festival programming as a direct result of feedback, we've made changes to the Library foyer, again following customer feedback, we've now launched an exciting new website and this will evolve and be enhanced further in the next few weeks.*
*We've asked the residents more questions about their needs and wants and now have a much clearer picture from our residents survey. A business survey is planned soon.*
*We've celebrated more Local Heroes at our event than ever before.*
*We've listened to the youth and now have an annual Youth Festival.*
*We are lobbying more services at Cornwall Council than ever before, to influence positive change, and we are talking to, and have relationships with more community groups than ever before.*
*We are also knocking on many more doors of businesses than ever before, with positive sponsorship results.*
*So, we are on a journey, we sincerely want to provide the best services we can but mutual honesty is critical, and trust, patience and collaboration is crucial on this journey. Distrust and impatience are prevalent, natural and expected, but I can assure you that each and every member of the team is 100% dedicated, committed and passionate about serving you all.*

DRAFT

*We look forward to continuing to work with you all.*
*You're all welcome to visit us at anytime at the Civic Centre. We are a front-facing team who all work very hard for the Redruth community.*
*Thank you.*

Cllr Broad continued the welcome to the meeting.

Cllr Broad introduced a series of speakers who informed the audience about their work in Redruth.

The Youth Council members talked about their aim to get more feedback from the young people in Redruth about what they want from the town, where they go and what services they need. The Youth Council is holding a stall in the Town Market on the first Saturday of each month and encourages any young person to talk to them about the issues and concerns that they would like to see addressed.

A local resident likened the friendliness of the Cornish people to those from his former home. He gave an impressive list of organisations in the town with which he is volunteering, including British Heart Foundation, Rise Up Redruth, Cornwall Air Ambulance, and the Town Council's Youth Festival as he stressed the importance of contributing to society.

The Bond Street Collective outlined their relationship with the Town Council which started off as being more or less non-existent but has developed in the last year. An initial meeting with the Town Clerk and Deputy Clerk last year has led to support from the Events Coordinator and Community Liaison Manager to enable the Collective to hold the Bond Street markets alongside the town festivals, including a very successful Redruth Pride event in June.

A volunteer outlined her work as a Digital Inclusion volunteer with the Library, helping people to access online services or deal with technology. This has helped people who may otherwise by digitally excluded to access Health Services online, which creates greater Health Equality in the town.

Bethel Community Larder described the support they have received from the Councillors who volunteer with them, which not only provides much-needed help but also allows the Councillors to hear first-hand about the issues that people are facing. They also acknowledged the work carried out by the Community Liaison Manager who is maintaining important dialogue across a range of organisations in the community and also thanked for the Council for the recent grant that enabled them to expand the facilities at the Larder.

Redruth Charity Trust described the work they are doing in the town, and they fact that they have donated £555,000 to local organisations since being formed. They are the only town charity trust in Cornwall. They have had a bumper year in terms of raising sponsorship from local people and businesses, and also described a good working relationship with the Town Council.

The Deputy Mayor opened the Q and A session, inviting questions from members of the audience.

A member of the public spoke warmly about the fact that the Councillors are volunteers, working to make Redruth a better place. He had particular praise for the hanging baskets and said he was looking forward to seeing how the Strategic Plan would unfold. He said that Redruth was on the up, and that people are investing in the town, so it was time to stay and be positive. He thanked the Town Council and staff for their hard work.

Representatives from the Banking Hub asked about the plan to establish a community Post Office in the town, as the Banking Hub offers many of the services that can be accessed via a post office, for example banking facilities, bill payments and utility card top-ups, access to pensions. They wanted to ensure that a community post office would not take away from what they are already doing.

The Town Clerk responded that the post office might offer other services such as the sale of stamps, and dealing with parcels but suggested the way forward was for the Council to work together with the Banking Hub to ensure any gaps were filled.

Cllr Thomas suggested that the desire for a town centre post office may be connected to the idea that it would be publicly owned.

Another member of the public queried the amount of cash that could be paid in at the Banking Hub counter as opposed to the post office. The limit depends on the framework that the post office is working to, but for the Banking Hub, it will be £8,000 when they move to permanent premises on Fore Street.

A local business owner stated that the Town Council meetings were a welcoming place for local people to go and raise issues with the Council and encouraged people to do so. Her experience was that issues had been dealt with well by Councillors and staff.

A question was raised about the future of the brewery site and the prospects of future development. Cllr Broad explained that the matter was complicated as the site was owned by an overseas investor.
Cllr Ellenbroek explained that as a former Cornwall Councillor, she and the other Cornwall Councillors at the time had worked hard with Cornwall Council and the site owner's agent to try to form a plan, but it was still a work in progress. She reiterated that if land is owned privately, there is very little the Tow Council or public can do. A Compulsory Purchase Order might be an option but there are lots of hoops to go through. She encouraged members of the public to contact the current Cornwall Councillors for Redruth on this matter and suggested that contacting them individually would be more effective than, for example, a petition.

There were no further questions and the formal part of the meeting closed at 19:45.

There followed an opportunity for members of the public to speak to Councillors and staff members individually about matters of interest to them, but this part of the meeting was not documented.

The meeting closed at 20:30.

**Town Mayor**

DRAFT

# Redruth Town Council
# Breach and Escalation Procedure

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

1. **DEFINITIONS**

The following definitions apply in this policy:

| | |
|---|---|
| **Council Representatives** | All officers, consultants, contractors, volunteers, interns, casual workers, agency workers of Redruth Town Council, along with Redruth Town Councillors (Members) and those with civic or ceremonial roles such as the Town Mayor and Town Crier of Redruth Town Council. |
| **Data Subject** | a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data. |
| **Breach** | any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Breach. |
| **Data Protection Officer** | Charlotte Williams |
| **ICO** | Information Commissioner's Office |
| **Personal Data** | any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes special categories of Personal Data (being information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data) and pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. |
| **UK GDPR** | UK General Data Protection Regulation |

## 2. POLICY BACKGROUND AND PURPOSE

2.1 This policy covers all Council Representatives (as defined above).

2.2 This policy does not form part of any employee's contract of employment and Redruth Town Council may amend it at any time.

2.3 Data breach is one of the most serious issues that public bodies face. Redruth Town Council is committed to securing all data that it is responsible for and that all staff share this responsibility. It is important that any breach is dealt with immediately and effectively.

2.4 This policy sets out how Redruth Town Council complies with the data protection legislation (including, but not limited to, the Data (Use and Access) Act 2025, UK GDPR and Data Protection Act 2018), confidentiality issues and information security requirements in the event of a loss of personal data.

## 3. APPLICATION AND RESPONSIBILITY

3.1 All Council Representatives must familiarise themselves and comply with this Policy and related procedures. Failure to comply with this Policy and the related procedures will result in disciplinary action. The serious nature of data breaches, the significant risks of fines, enforcement action, reputational damage and disciplinary action, means that everyone in the organisation must play a part in compliance.

3.2 All Council Representatives are responsible for ensuring that all types of data are properly protected and kept secure.

3.3 Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action (for employees) or Code of Conduct investigations (for applicable Council Representatives). In the case of a breach of this policy by a volunteer, contractor, consultant, casual or agency worker, the immediate termination of the engagement.

## 4. DATA PROTECTION AND GDPR

4.1 Both data controllers and data processors must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Failure to do so can result in individuals losing control of their personal information. The UK GDPR also allows for the ICO to issue fines of up to €20m (£17.5m) or 4% of annual turnover, whichever is greater. In addition, there would also be a detrimental effect to Redruth Town Council's reputation from any negative press and increased operating costs after the fine.

## 5. DATA SECURITY BREACH OR POTENTIAL LOSS OF PERSONAL DATA

5.1 If a Council Representative becomes aware of any:

- loss or potential loss of personal data;
- breach or potential breach of confidentiality;
- loss of laptop, tablet or other device, e.g. smartphone or mobile phone (whether it belongs to Redruth Town Council or to a Council Representative personally), which may result in a loss of data or breach of confidentiality;
- breach of information security, whether physical or electronic;

the Council Representative must immediately inform the Data Protection Officer so that appropriate action can be taken and serious breaches reported. Where possible, the Council asks Council Representatives to complete a Breach Form and appendix A. If a report needs to be made out-of-hours, you must contact the Town Clerk. In the case of a breach relating to Redruth Library operations or activities the member of staff must also follow the procedures of Cornwall Council.

5.2 To enable the Data Protection Officer to determine whether the breach is serious, the Council Representative must provide all relevant information as requested by Data Protection Officer and assist with the Data Protection Officer's assessment. The Data Protection Officer may use the *Breach Risk Assessment* document to perform the necessary assessment, although this is not mandatory.

5.3 On receipt of the report, the Data Protection Officer will respond to the incident and manage all communication. Under no circumstances should a Council Representative engage in communication with another Council Representative or any third party in relation to the breach. Specifically, Council Representatives must not report a breach to the ICO unless they have been directed to do so in writing by the Data Protection Officer.

5.4 The Council have provided illustrative examples of data breaches in Annex B of this Policy.

## 6. FOIA/EIR BREACHES

6.1 Where a Council Representative becomes aware of any actual or potential breach relating to the handling of requests under the Freedom of Information Act 2000 (**FOIA**) or the Environmental Information Regulations 2004 (**EIR)**, they must notify the Data Protection Officer immediately. In the case of a breach relating to Redruth Library operations or activities the member of staff must also follow the procedures of Cornwall Council.

7. A FOIA/EIR breach may include, but is not limited to:

7.1.1 Failure to respond to a request within the statutory timeframe (in most cases 20 working days);

7.1.2 Unauthorised disclosure of exempt or sensitive information;

7.1.3 Accidental disclosure of information to the wrong requester;

7.1.4 Loss or compromise of information relevant to a live FOIA/EIR request;

7.1.5 Failure to apply the correct exemptions/exceptions;

7.1.6 Any security incident affecting information subject to a request.

8. The Data Protection Officer will assess the breach and determine appropriate next steps. Council Representatives must not communicate with the requester or any third party about the breach unless instructed to do so in writing by the Data Protection Officer.

9. Where appropriate, the DPO will liaise with the Town Clerk (if a separate person) and any other relevant officers to:

9.1.1 Contain the breach and recover any disclosed information where possible;

9.1.2 Assess the impact on individuals, the Council, and statutory obligations;

9.1.3 Determine whether the ICO must be notified; and

9.1.4 Ensure any required correspondence with the requester is accurate, timely, and legally compliant.

10. The Data Protection Officer will also consider whether the incident highlights whether additional training, guidance or procedural improvements are required.

## 11. ESCALATION PROCEDURE

<u>Containment and Recovery</u>

11.1 The Data Protection Officer will:

11.1.1 Investigate the breach in conjunction with, and/or with assistance from, such individuals (including Council Representatives) and third parties as necessary, and ensure they have appropriate resources to properly investigate the breach;

11.1.2 Establish who needs to be made aware of the breach and inform them of what they must do to assist in any containment action required. Where the breach impacts the Library, the Town Clerk must ensure that any contractual requirement to inform Cornwall Council is fulfilled. Library Staff must not make a report to Cornwall Council without first seeking the approval of the Town Clerk;

11.1.3 Establish whether anything can be done to recover any lost data and for to limit the damage caused by the breach;

11.1.4 Identify any third party involved in the breach and liaise with them, as appropriate; and

11.1.5 Where appropriate, inform the relevant law enforcement agencies and the ICO.

Preservation of evidence

11.2 Council Representatives must preserve all logs, screenshots or audit trails that would assist the Data Protection Officer, and any regulator, when investigating the incident. This requirement takes precedent over any retention period set out within the Data Retention Policy.

11.3 Council Representatives are not permitted to delete emails or data connected to any breach.

Assessing the Risks

11.4 The Data Protection Officer will assess the risks which may be associated with the breach before taking any steps after the immediate containment, as follows:

11.4.1 What type of data is involved?

11.4.2 How sensitive is the data?

11.4.3 If the data has been lost or stolen, is there any protection, e.g. encryption?

11.4.4 What has happened to the data?

11.4.5 How could the data be misused?

11.4.6 How many individuals are affected?

11.4.7 Who are the individuals affected?

11.4.8 What harm can come to those individuals as a result of the loss / breach?

11.4.9 How serious / substantial is the harm?

11.4.10 How likely is it that any harm will happen?

11.4.11 Are there wider consequences to consider?

11.4.12 If an individual's bank details have been lost, what steps can be taken to prevent fraud?

11.5 Depending on the conclusion the Data Protection Officer will decide who needs to be notified.

Notification of Breaches

11.6 The UK GDPR requires Controllers to notify any personal data breach which is likely to cause a risk to the rights and freedoms of individual to the Information Commissioner. Where the risk is high, the Data Subject must also be informed.

11.7 The Council has 72-hours from “becoming aware” of the Breach to make the legally mandated reports. This is why immediate reporting to the Data Protection Officer is vital.

11.8 The Data Protection Officer will consider the following in determining whether (and who) to notify:

11.8.1 legal / contractual requirements (such as Cornwall Council).

11.8.2 Will notification help to meet the obligation to report in relation to the UK GDPR?

11.8.3 Can notification help the individual?

11.8.4 Once we have established the severity of the resulting risk to people’s rights and freedoms, the ICO can be informed.

11.8.5 How notification can be made appropriate for particular groups of individuals, e.g. vulnerable adults.

11.8.6 The dangers of over-notifying.

11.9 The Data Protection Officer will consider the above before deciding who to notify, what information to provide and how the information is to be communicated.

11.10 Any decision to report to the insurers, the ICO or Data Subjects (and what information to provide) will be taken by the Data Protection Officer.

<u>Evaluation and Response Phase</u>

11.11 The Data Protection Officer will evaluate the effectiveness of Redruth Town Council’s response to the breach by considering the following:

11.11.1 What was the cause of the breach / reason for the loss?

11.11.2 What steps can be taken to prevent a recurrence?

11.11.3 Was the response hampered by inadequate policies or a lack of a clear allocation of responsibility?

11.11.4 Could existing procedures lead to another breach?

11.11.5 Where can improvements be made to the systems and controls?

11.12 The Data Protection Officer should ensure that they:

11.12.1 Complete the Data Breach Log;

11.12.2 Know what personal data is held, where and how it is stored;

11.12.3 Establish where the major risks are and why, how much sensitive personal data is held, is data stored across the business or concentrated in one location;

11.12.4 Consider the risks involved in sharing data with or disclosing data to others; whether the method of transmission is secure; whether the

minimum amount of data being shared / disclosed which data controllers / data processors / third parties Redruth Town Council shares with and whether the contracts need to be amended / improved;

11.12.5 Identify weak points in the existing security measures such as the use of portable storage devices;

11.12.6 Monitor Council Representatives' awareness of security issues and address any gaps through training or tailored advice;

11.12.7 Consider whether to establish a working group of Council Representatives to discuss "what if" scenarios to highlight risks and weaknesses and provide an opportunity for Council Representatives to suggest solutions;

11.12.8 Consider if National Cyber Security Centre (NCSC) needs to be informed (where breach is caused by suspicious online actors or websites);

11.12.9 Implement and test a Business Continuity Plan for data security breaches; and

11.12.10 Identify a group of people responsible for reacting to reports of breaches of security or significant data loss.

## 12. GUIDANCE

12.1 The Data Protection Officer must be aware of the requirements of Information Commissioner Guidance on personal data breaches: Personal data breaches: a guide | ICO.

**Appendix A – Breach Form**

# Redruth Town Council
# Breach and Escalation Procedure Form

Adopted: October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

This form is for Council Representatives to report personal data breaches to the Data Protection Officer.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

## 1. REPORT

Please answer the following questions, to help us handle your report efficiently.

- Please describe what happened
- Please describe how the incident occurred
- How did you discover the breach?
- What preventative measures did you have in place?
- Was the breach caused by a cyber incident?
- When did the breach happen?

  Date: Time:

- When did you discover the breach?

  Date: Time:

- Categories of personal data included in the breach (tick all that apply)

  - ☐ Data revealing racial or ethnic origin
  - ☐ Political opinions
  - ☐ Religious or philosophical beliefs
  - ☐ Trade union membership
  - ☐ Sex life data
  - ☐ Sexual orientation data
  - ☐ Health data
  - ☐ Basic personal identifiers, eg name, contact details
  - ☐ Identification data, eg usernames, passwords
  - ☐ Economic and financial data, eg credit card numbers, bank details
  - ☐ Official documents, eg driving licences

- ☐ Location data, eg coordinates
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Other (please give details below)

- Please give additional details to help us understand the nature of the personal data included in the breach:

- Number of personal data records concerned?

- How many data subjects could be affected?

- (Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected
- Categories of data subjects affected (tick all that apply)

  - ☐ Employees, adult volunteers or Workers
  - ☐ Councillors, Mayor or Town Crier
  - ☐ Public
  - ☐ Suppliers (and their employees)
  - ☐ Children
  - ☐ Vulnerable adults
  - ☐ Other (please give details below)

- Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future
- Is the personal data breach likely to result in a high risk to data subjects?

  - ☐ Yes
  - ☐ No
  - ☐ Don’t know - please give details:

- Recovery / Mitigating Actions (Tick all that apply):

  - ☐ You have successfully recalled or retrieved information
  - ☐ You have been able to confirm that information has been deleted
  - ☐ You have back-up information
  - ☐ You have changed passwords or access credentials on affected systems
  - ☐ You have restricted or suspended access to systems or accounts
  - ☐ You have isolated the incident or taken steps to secure information
  - ☐ Other:

- If the breach relates to a suspicious website, please provide the URL in plain text:

**PERSON MAKING THIS REPORT**

- Name:
- Email:
- Phone:
- Role:
- Date:

## Appendix B – Breach Examples

1.1 The following examples are intended to help Council Representatives identify situations which may amount to an actual or potential personal data breach. They are illustrative only. If there is any doubt, the matter must be reported to the Data Protection Officer immediately so that it can be assessed.

- A Council Representative emails a spreadsheet containing residents' names, addresses, telephone numbers and complaint details to the wrong recipient.
- A letter about is posted to the wrong address.
- A member of staff attaches the wrong file to an email, disclosing another person's personal information.
- A paper file containing staff records, volunteer details, DBS information, recruitment documents or sickness absence information is left in a public area, meeting room, printer tray, library counter or vehicle.
- A laptop, tablet, mobile phone, USB stick, access card or paper notebook containing Council or library information is lost or stolen.

- A Council Representative discusses information relating to a member of the public, resident, staff member, volunteer, councillor or library user in a public area where the conversation can be overheard.
- An email is sent to multiple people using the “To” or “Cc” field instead of “Bcc”, revealing email addresses to other recipients.
- A FOIA or EIR response is sent to a requester without removing personal data, commercially sensitive material, safeguarding information, or information which should have been withheld under an applicable exemption or exception.
- A subject access response includes another person’s personal data because redactions were missed or applied incorrectly.
- CCTV footage is shared with an unauthorised person, retained for longer than permitted, downloaded to an unsecured device, or viewed by someone without a legitimate reason.
- Library membership information, borrowing history, reservation details, computer booking records or enquiry notes are disclosed to another person without proper authority.

- A library user's account is left open on a shared computer or staff terminal, allowing another person to view or amend their personal information.
- A volunteer or contractor is given access to more information than they need for their role, or retains access after their work for the Council or library has ended.
- An online form, booking system, survey platform or shared drive is configured incorrectly, allowing members of the public or unauthorised staff to view personal information submitted by others.
- A phishing email is opened and login details are entered, giving an unauthorised person potential access to Council or library systems.
- An employee forwards Council or library emails to a personal email account, or stores Council information on a personal device or personal cloud storage without approval.
- Printed agendas, minutes, complaint papers, HR papers or safeguarding records are disposed of in general waste rather than confidential waste.

- A member of staff gives information about a library user, resident or service user to a family member, neighbour, councillor or third party without checking whether disclosure is lawful and authorised.

- A social media post, website update or newsletter includes a photograph, name, address, contact details or other identifiable information without the necessary authority, lawful basis/consent or checks.

- A cyber incident, ransomware attack or unauthorised access attempt affects Council or library systems which contain personal data, even where it is not yet clear whether information has been viewed or extracted.

- A Councillor or Officer breaches Part 2 confidentiality rules

# Redruth Town Council
# Bring Your Own Device (BYOD) Policy

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## 1. INTRODUCTION

1.1 Redruth Town Council (**"the Council", "we" or "us"**) recognise that there may be extremely limited circumstances when Council Representatives may be granted the authority to use personal mobile devices for business purposes. **This permission shall only be granted in exceptional circumstances and solely at the discretion of the Town Clerk (such permission to be in writing).**

1.2 For the avoidance of doubt, this policy does not capture use of Cornwall Council devices.

1.3 The purpose of this policy is to set out the rules of using personal mobile devices for Council purposes (where you are granted authority by the Town Clerk) and how this policy should be adopted to minimise security risks or concerns when you access our systems using a device.

1.4 We do not require or force Council Representatives to use personal mobile devices for work, it is a matter of personal discretion. This policy applies to Council Representatives who use a personal mobile device for Council purposes, both during and outside office hours, whether or not used at your normal place of work.

1.5 This policy should be read in conjunction with our other policies and procedures in place, including our Officer and Member Privacy Policy and Data Retention Policy, which are available from HR.

1.6 This policy does not form part of any contract of employment or contract to provide services, and we may amend or remove the policy at any time.

## 2. DEFINITIONS

2.1 The following definitions in this policy:

| | |
|---|---|
| **Council Data** | information about us, our clients and other Council connections, whether confidential, proprietary or private, held, used or transmitted in any forms including written, spoken and electronically. |
| **Council Representatives** | all officers, consultants, contractors, volunteers, interns, casual workers, agency workers of Redruth Town Council, along with Redruth Town Councillors (Members) and those with civic or ceremonial roles such as the Town Mayor and Town Crier of Redruth Town Council. |
| **Content** | any materials, information and communications including but not limited to email (both outgoing and |

| | |
|---|---|
| | incoming), telephone conversations, voicemail recordings, instant messages and social media postings, created, transmitted, received, printed, stored or recorded during the course of Council business or on our behalf. |
| **Device** | a smartphone, tablet, handheld computer, and any accompanying software or hardware. |
| **Personal Data** | any information relating to an identified or identifiable natural person, be it directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **Systems** | the Council's IT, communications and information systems. |

## 3. PERSONNEL RESPONSIBLE FOR THIS POLICY

3.1 The Town Clerk and the DPO shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

3.2 Team Managers or Leaders also have responsibility for ensuring that any person who may be involved with administration, monitoring, IT security or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

3.3 All Council Representatives are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the Town Clerk and DPO.

## 4. SCOPE OF THIS POLICY

4.1 When Council Representatives access our systems using a device, we are exposed to a number of risks which could result in damage to our systems, the Council and our reputation:

4.1.1 loss or theft of the device, resulting in unauthorised access to our systems or Council Data;

4.1.2 threat of malware, such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device; and

4.1.3 loss or unauthorised alteration of Council data, which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy).

4.2 This policy sets out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

4.3 Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action (for employees) or Code of Conduct investigations (for applicable Council Representatives). In the case of a breach of this policy by a volunteer, contractor, consultant, casual or agency worker, the immediate termination of the engagement. It may also lead in some cases to possible criminal charges.

4.4 For the avoidance of doubt, disciplinary action or Code of Conduct investigations may be taken whether the breach is committed during or outside office hours and whether or not use of the device takes place at your normal place of work.

4.5 Where we are required to investigate into a suspected breach, we ask for your co-operation with any investigations, which may involve providing us with access to your device, any relevant passwords and login details.

## 5. DUTY TO LIMIT

5.1 Council Representatives are under a duty to minimise their use of personal devices. Where a Council has issued a device and this device is available/suitable for use, the Council-maintained device must be used in preference to any personal device.

## 6. CONNECTING DEVICES TO OUR SYSTEMS

6.1 Connectivity of all devices is centrally managed by our external IT support provider, which must approve a device before it is connected to our systems. Only in exceptional circumstances shall the Town Clerk permit use of personal devices for work purposes, acting in consultation with our external IT support provider, will have full discretion to approve or reject the device.

6.2 Before using your device to connect to our systems, or to access Council Data, in accordance with this policy, you must:

6.2.1 inform and register your device with the Town Clerk; and

6.2.2 implement technical security measures as the external IT support provider may reasonably require.

6.3 You are not permitted to use any device other than the device that has been registered and approved by us. We reserve the right to refuse or remove permission for your device to connect with our systems. The Town Clerk may refuse or revoke such permission (and may take all steps reasonably necessary to do so), where in their reasonable opinion a device is or could be used in a way that puts us, our Council Representatives, our connections, our systems, or our Council Data at risk or that may otherwise breach this policy.

6.4 In order to access our systems, it may be necessary for our external IT support provider to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

6.5 Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist Council Representatives in connecting to our systems in that case.

## 7. MONITORING

7.1 Regardless of ownership of the device, the contents of our systems and Council Data are our property.

7.2 We reserve the right to conduct reasonable and proportionate monitoring, interception, reviews and erasures, without further notice, all content on the device that has been created for us or on our behalf. This might situations where:

7.2.1 we are investigating a suspected breach of Council policy or legal obligation;

7.2.2 we must action to safeguard the security or integrity of Council systems or information assets; or

7.2.3 we must comply with a legal or regulatory requirement.

7.3 Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, in order for us to comply with a legal obligation or for our legitimate Council purposes, including, without limitation, in order to:

7.3.1 prevent misuse of the device and protect Council Data;

7.3.2 ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy); and

7.3.3 ensure that Council Representatives members do not use our facilities or systems for any unlawful purposes or activities that may damage the Council or reputation.

7.4 Any monitoring or access will be limited strictly to information that is relevant to the identified purpose. The Council will not access personal data stored on the device unless this is unavoidable in the circumstances and necessary to achieve the stated purpose.

7.5 The Council will not undertake continuous or generalised monitoring of personal devices. Intrusive monitoring techniques shall be avoided, save where exceptional circumstances, authorised by the Town Clerk, arise.

7.6 Where the Council needs to review or retrieve Council Data from a device, it will take reasonable steps to minimise access to personal data, and to avoid copying or retaining personal data contained on the device.

7.7 Council Representatives must co-operate with proportionate access measures if required for a specific and identified purpose under this policy.

## 8. SECURITY REQUIREMENTS

8.1 When using your device for any Council purposes, you must comply with the requirements as listed below. You must:

8.1.1 at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you;

8.1.2 install any antivirus or antimalware software at our request before connecting to our systems and consent to our efforts to manage the device and secure its data, including providing us with any necessary passwords;

8.1.3 comply with our device configuration requirements;

8.1.4 protect the device with a PIN number or strong password, and keep that PIN number or password secure at all times. The PIN number or password should be changed regularly. If the confidentiality of a PIN number or password is compromised, you must change it immediately. The use of PIN numbers and passwords should not create an expectation of privacy by you in the device;

8.1.5 maintain the device's original operating system and keep it current with security patches and updates. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing out systems or Council Data;

8.1.6 not download and install software to the device unless explicitly authorised by us;

8.1.7 not download or transfer any Council Data to the device, for example via e-mail attachments, unless specifically authorised to do so. Council Representatives must immediately erase any such information that is inadvertently downloaded to the device;

8.1.8 not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of Council Data. Any such backups inadvertently created must be deleted immediately;

8.1.9 not use public unsecured Wi-Fi to access our systems without our prior consent; and

8.1.10 not sell, replace or transfer the device to anyone else without our prior consent.

8.2 We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the Council Data on it for legitimate Council purposes, which include (without limitation) enabling us to:

8.2.1 inspect the device for use of unauthorised applications or software;

8.2.2 inspect any Council Data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect Council Data;

8.2.3 investigate or resolve any security incident or unauthorised use of our systems;

8.2.4 conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and

8.2.5 ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

8.4 You must co-operate with us to enable such inspection, access and review, including providing any passwords or PIN numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal, Code of Conduct investigation or, where applicable, termination of any non-employment relationship.

8.5 If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we may immediately remove your access to our systems and, where appropriate, remove any Council Data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from Council Data in all circumstances. You should therefore regularly backup, and keep separate, any personal data contained on the device.

## 9. LOST OR STOLEN DEVICES AND UNAUTHORISED ACCESS

9.1 In the event of a lost or stolen device, or where a device is suspected of being accessed by an unauthorised person or otherwise compromised, this must be reported to the Town Clerk and the DPO immediately.

9.2 We take appropriate steps to ensure that Council Data on the device is secured, including where reasonable and reasonable and proportionate, remotely wiping the device where appropriate. This will destroy all Council

Data on the device (including information contained in a work email account, even if such e-mails are personal in nature).

9.3 Although we do not intend to wipe other data that is strictly personal in nature (such as photographs, personal files or emails), it may not be possible to distinguish all such information from Council data in all circumstances. You should therefore regularly backup, and keep separate, all personal data stored on the device.

## 10. PROCEDURE ON DEPARTURE OR AND SELLING, TRANSFERRING OR REPLACING THE DEVICE

10.1 On you last day prior to departure from the Council (termination of employment or expiry of officeholding, volunteer post or contractor arrangement), or your last day before commencing a period of extended leave, or when you intend to sell or transfer your device to anyone else, all Council Data and software applications provided by us for Council purposes must be removed from the device and all Council Data returned to the Council. The Town Clerk (and any external IT support provider) will assist with this process. If this cannot be achieved remotely, we may ask you to submit your device to the Council for wiping and software removal. We ask for your co-operation and assistance in completing this process.

## 11. PERSONAL DATA

11.1 We have a legitimate basis on which to access and protect Council Data stored or processed on your device. However, we recognise the need to balance our obligation to process data for legitimate purposes, with your expectations of privacy in respect of your personal data. Therefore, if we need to access your device or delete data on your device, remotely or otherwise, in accordance with this policy, we will:

11.1.1 consider whether the action is proportionate in light of the potential damage to the Council, the public or other people impacted by Council Data;

11.1.2 consider if there is an alternative method of dealing with the potential risks to the Council's interests;

11.1.3 take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur; and

11.1.4 delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data which is also Council Data, including all personal emails sent or received using our email system).

11.2 To reduce the likelihood of the Council inadvertently accessing your personal data, or the personal data of third parties, you must comply with the following steps:

11.2.1 organise files within the device specifically into designated folders that clearly distinguish between Council Data and personal data (for example, marking Council folders as "RTC: [folder name]");

11.2.2 ensure any ‘chat’ streams for Council purposes (such as Council events) are clearly distinguished by a tag “RTC: [chat name]”;

11.2.3 refrain from using any form of personal email unless permitted by the Town Clerk. Where permitted, your work-related emails (sent and received) should be stored within a clearly distinguishable folder marked “RTC Emails”; and

11.2.4 refrain from using your work email for personal purposes.

11.3 Please ensure any Council Data is retained in accordance with our Retention Policy.

## 12. APPROPRIATE USE

12.1 Before using your device under this policy for the first time, you must erase all information and software related to any previous employment. You may be asked to confirm to us that this has been done.

12.2 You must ensure that Council Data is used only for the Council purposes for which it was originally intended, and that you do not use it for a different purpose. For example, you should not use contact information gathered for Council purposes for your own personal purposes. You should also minimise the amount of Council Data you retain on the device by accessing information remotely where possible, and deleting any data saved locally on your device as soon as it is no longer required.

12.3 You should never access or use our systems or Council Data through a device in a way that breaches our legal obligations or any of our other policies. For example:

12.3.1 breach our obligations with respect to the rules of relevant regulatory bodies, in particular in relation to confidentiality and privacy;

12.3.2 breach any other laws or ethical standards (for example, the Code of Conduct, Civility and Respect Pledge);

12.3.3 defame or criticise us or our affiliates, Council Representatives, members of the public, partners, suppliers, vendors or other stakeholders; or

12.3.4 harass, bully or discriminate against other Council Representatives or third parties in any way.

12.4 You must not use a device in any way, be it talk, text, email or otherwise, while operating any vehicle for Council purposes. You must comply with any applicable laws concerning the use of devices in vehicles.

## 13. TECHNICAL SUPPORT

13.1 The Town Clerk and the Council's external IT support provider will provide technical support in setting up your device for Council use and assist in resolving any issues that arise during the set up and use of the device.

13.2 If the issue relates to the software we provide, we will provide all necessary support. However, if the issue is hardware related or relates to software which you have installed personally, then you will be responsible for fixing it, including any repairs, maintenance or replacements incurred.

## 14. COSTS AND REIMBURSEMENTS

14.1 Unless agreed otherwise, you are responsible for all costs associated with your device, including all voice and data usage, purchase and repair costs.

## 15. CHANGES TO THIS POLICY

15.1 We keep our Bring Your Own Device (BYOD) Policy under regular review. This version was last updated in October 2026.

# Redruth Town Council
# Retention Policy

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## 1. ABOUT THIS POLICY

1.1 The corporate information, records and data of Redruth Town Council is important to how we perform our public function and relationship with **Council Representatives**, defined as all officers, consultants, contractors, volunteers, interns, casual workers, agency workers of Redruth Town Council, along with Redruth Town Councillors (Members) and those with civic or ceremonial roles such as the Town Mayor and Town Crier of Redruth Town Council

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our organisation operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well unnecessary cost.

1.3 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.5 This policy has been agreed following consultation with Members of Redruth Town Council.

1.6 This policy does not form part of any Council Representative's contract of employment, and we may amend it at any time.

## 2. SCOPE OF POLICY

2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by Council Representatives on personal devices in accordance with our BYOD Policy.

2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

2.4 This policy applies to all departments and all Redruth Town Council functions.

## 3. GUIDING PRINCIPLES

3.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate Redruth Town Council effectively, but we do not create or retain data without good reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind all Council Representatives of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

## 4. ROLES AND RESPONSIBILITIES

4.1 **Responsibility of all Council Representatives**. We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All Council Representatives must comply with this policy, the Record Retention Schedule, any communications suspending data disposal and any specific instructions from the Records Management Officer, Town Clerk or DPO. Failure to do so may subject us, our Council Representatives, and contractors to serious civil and/or criminal liability. A Council Representative's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination, or in the case of Members, an investigation under the Code of Conduct. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 We have designated Sarah Brown as the Records Management Officer. The Records Management Officer is a person designated to ensure proper records management and is responsible for:

- Administering the data management programme;
- Helping department heads implement the data management programme and related best practices;
- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and
- Providing guidance, training, monitoring and updating in relation to this policy.

4.3 **Data Protection Officer.** Our Data Protection Officer (DPO) is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. Our DPO works with our Records Management Officer on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data.

## 5. TYPES OF DATA AND DATA CLASSIFICATIONS

5.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to our public task. Please see paragraph 6.1 below for more information on retention periods for this type of data.

5.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Redruth Town Council and retained primarily for reference purposes.

- Spam and junk mail;

Please see paragraph 6.2 for more information on how to determine retention periods for this type of data.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (the principle of storage limitation) (see paragraph 6.3 for more information on this).

5.4 **Confidential information belonging to others**. Any confidential information that Council Representative may have obtained from a source outside of Redruth Town Council, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

5.5 **Data classifications.** Some of our data is more confidential than other data, in contract to this, some of our information must be published under our Publication Scheme. We take clear steps to classify data (including personal data) and will communicate how each type of data should be marked and protected.

## 6. RETENTION PERIODS

6.1 **Formal or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, or if you believe an exception should be made to allow a record to be retained for longer than the amount of time indicated in the Record Retention Schedule, contact the Records Management Officer.

6.2 **Disposable information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for Council purposes. Once it no longer has any Council purpose or value it should be securely disposed of.

6.3 **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record

Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data. More information can be found in in our Internal Data Protection Policy or by contacting the DPO.

6.4 **What to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, and it is unlikely to constitute disposable information, you must immediately inform the Record Management Officer.

## 7. STORAGE, BACK-UP AND DISPOSAL OF DATA

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our operations during an emergency must be duplicated and/or backed up at least once per day and maintained off site.

7.2 **Destruction**. Our Records Management Officer is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and Council Representative-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with the relevant outsourced IT support team, with the relevant back-up systems being considered during the destruction process. Please note that deletion from back-up systems may not always be technically possible or fully effective.

7.3 The destruction of data must stop immediately upon notification from any person that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the Records Management Officer lifts the requirement for preservation.

## 8. SPECIAL CIRCUMSTANCES

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all Council Representatives to comply fully with our Record Retention Schedule and procedures as provided in this policy. All Council Representatives should note the following general exception to any stated destruction schedule: If you believe, or anyone informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those

records, including emails and other electronic documents, until the Records Management Officer determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Records Management Officer immediately.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

## 9. ARCHIVED PUBLIC RECORDS

9.1 Archived records are maintained in line with our retention policy.

## 10. FOIA AND EIR 'LIVE' REQUESTS

10.1 Redruth Town Council must not destroy information subject to an ongoing 'live' request under the Data Rights and Information Access Policy (Data Rights, FOIA or EIR requests). Such information shall also be subject to a prohibition on altering information after it has become subject to an FOI request. Failure to meet this obligation may constitute an offence.

10.2 The destruction of data must stop immediately upon notification from any person that preservation of documents for Data Rights or FOIA/EIR purposes. Destruction may begin again once the Records Management Officer lifts the requirement for preservation.

## 11. WHERE TO GO FOR ADVICE AND QUESTIONS

11.1 **Questions about the policy.** Any questions about retention periods relevant to your department should be raised with your department manager in the first instance. Any questions about this policy should be referred to the Records Management Officer, who is in charge of administering, enforcing, and updating this policy.

## 12. BREACH REPORTING AND AUDIT

12.1 **Reporting policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depend largely on Council Representatives. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your

supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the Records Management Officer. If Council Representatives do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

12.2 No one will be subject to and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

12.3 **Audits**. Our Records Management Officer, and any duly authorised external third-party auditor, will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

## 13. OTHER RELEVANT POLICIES

13.1 This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our IT, security and data related policies, which are available on our website.

## ANNEX A DEFINITIONS

**Data:** all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

**Data Protection Officer:** our Data Protection Officer who is responsible for advising on and monitoring compliance with data protection laws.

**Data Retention Policy:** this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

**Disposable information**: disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule.

**Formal or official record:** certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

**Non-personal data:** data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

**Personal data:** any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**Records Management Officer:** the Records Management Officer is responsible for administering the data management programme, helping department heads implement it and related best practices, planning, developing, and prescribing data disposal policies, systems, standards, and procedures and providing guidance, training, monitoring and updating in relation to this policy.

**Record Retention Schedule:** the schedule attached to this policy which sets out retention periods for our formal or official records.

**Storage limitation principle:** data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the UK GDPR and EU GDPR as the principle of storage limitation.

## ANNEX B RECORD RETENTION SCHEDULE

Redruth Town Council establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Council Representatives should comply with the retention periods listed in the record retention schedule below, in accordance with the Redruth Town Council Data Retention Policy.

The schedule below should be read with the ACSS Town and Parish Councils document retention schedule and guidance 2025. Where the ACSS schedule covers the same or equivalent category, the ACSS retention period and final action have been amalgamated below. Records marked “Preserve” should be retained locally for the stated minimum period and then transferred to Kresen Kernow, unless there remains an administrative requirement to retain them locally. Records marked “Destroy” should be securely destroyed at the end of the stated period, subject to any litigation hold, audit, FOIA/EIR request hold, data rights request hold, or other legal requirement requiring continued preservation.

If you hold data not listed below, please refer to the Redruth Town Council Data Retention Policy. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this record retention schedule, please contact the Records Management Officer.

**Council Records**

| Description | Retention Action | Examples of Records | Reason for retention |
|---|---|---|---|
| Council & Committee Meetings | Retain in Council custody for 4 years from the date of the last entry, then preserve and transfer to Kresen Kernow. Agendas should not be retained unless they contain significant information not in the minutes | Council minutes<br>Council agenda and business papers<br>Council notice papers and proceedings<br>Indexes<br>Committee minutes | ACSS Town and Parish Councils document retention schedule and guidance 2025 |

| | | | |
|---|---|---|---|
| | or the minutes do not exist. | | |
| Minute taking | Destroy after date of confirmation of the minutes | Draft/rough minutes or recordings | |
| Partnership, Agency, and External Meetings | Where RTC legally owns the record and it comprises minutes, reports or significant papers associated with Council decisions, retain for 4 years from the date of the last entry, then preserve and transfer to Kresen Kernow. | Documents establishing the committee.<br>Agendas<br>Minutes<br>Council reports<br>Recommendations<br>Supporting documents e.g., council briefings and discussion papers | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Partnership, Agency, and External Meetings | Where RTC does not own the record, retain only for administrative need. If retained as routine correspondence or supporting papers not requiring preservation, retain for 4 years from the date of last action, then destroy. | Reports<br>Recommendations<br>Supporting documents | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Register of Interests | Destroy 12 months after | | ACSS Town and Parish Councils |

| | | | |
|---|---|---|---|
| | the Councillor or Member ceases role. | | document retention schedule and guidance 2025 |

**Management & Administration**

| | | | |
|---|---|---|---|
| Corporate planning and reporting activities of local authorities | Retain for 4 years from the date of the last entry, then preserve if the record is a town/parish plan, appraisal, report or significant policy record documenting major local decisions or developments. Otherwise retain for administrative need and review before destruction. | Corporate plans<br>Strategy plans<br>Business plans<br>Annual reports | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Process of preparing business for strategic consideration and making the record of discussion, debate, and resolutions | | Strategic management team minutes | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Statutory returns – the process of preparing information to be passed on to central government as part of statutory requirements | Retain for 4 years from submission of the final return, or closure of the matter to which the return relates, whichever is later, then destroy. Where the return is financial, audit, tax or grant-related, retain for 7 years. | Reports to central government | ACSS Town and Parish Councils document retention schedule and guidance 2025 |

| | | | |
|---|---|---|---|
| | Where the return evidences a significant council decision, major development, governance matter or matter of enduring public interest, review for preservation before destruction | | |
| Policy, Procedures, Strategy and Structure | Retain for 4 years from the date of the last entry, then preserve where the record documents significant Council policy, governance, major developments or decisions. Routine administrative policy working papers should be retained for 4 years, then destroyed. | Policy, procedure, precedent, instructions<br>Organisation charts<br>Records relating to policy implementation and development.<br>Education plan<br>Asset management plan<br>Community strategy<br>Community plan<br>Community safety plan | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Draft Policy, Procedures, Strategy and Structure | Destroy 7 years after administrative use is concluded | Draft policy, procedure, precedent, instructions<br>Draft organisation charts<br>Draft records relating to policy implementation and development. | |

| | | | |
|---|---|---|---|
| | | Draft asset management plan<br>Draft community strategy | |
| Public Consultation – significant policies | Destroy 5 years from closure | Feasibility studies/surveys | |
| Public Consultation – minor policies | Destroy 1 year from closure | Festival feedback | |
| Enquiries and Complaints | Routine enquiries and complaints: retain for 4 years from last action, then destroy.<br>Significant correspondence relating to major developments or Council decisions should be retained for 4 years, then preserve. | Reports<br>Correspondence<br>Letters | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Quality and Performance Management – process of monitoring the quality, efficiency or performance of a local authority service or unit | Destroy 5 years from closure | Best Value Review Assessment Form | |
| Publications – published work of the local authority | Retain town/parish magazines, newsletters, histories, scrapbooks, captioned | Marketing materials e.g., posters and flyers | ACSS Town and Parish Councils document retention schedule and guidance 2025 |

| | | | |
|---|---|---|---|
| | photographs and publicity material for 4 years, then preserve or sample if large in number. Press cuttings, objects and memorabilia should not be transferred to Kresen Kernow. | | |
| Media Relations – media publications concerning local authorities | Do not retain press cuttings permanently for transfer. Retain only for administrative need or where incorporated into a wider preserved record, then destroy. | Press cuttings<br>Media reports | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Marketing – developing and promotion of local authority campaigns and events | Retain publicity material for 4 years, then preserve or sample if large in number. Routine promotional material with no enduring value should be destroyed when no longer required. | | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Photographs | Retain identifiable, dated and captioned | Only relevant to photographs that have been identified and dated to be useful in the future | ACSS Town and Parish Councils document |

| | | | |
|---|---|---|---|
| | photographs for 4 years, then preserve or sample if large in number. Routine or unidentified images should be destroyed when no longer required. | | retention schedule and guidance 2025 |
| Civic and Royal Events – recording of ceremonial events and civic occasions | Retain records of significant civic or ceremonial events for 4 years, then preserve or sample if large in number. Video or sound recordings should be weeded, sampled and digitised before transfer. | Visitors book<br>Audio tapes<br>Video tapes<br>Photographs | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Organising a ceremonial event or civic occasions (including Financial Information) | Destroy 7 years after administrative use is concluded | If an RTC arranged event, then please keep one copy of the invitation/correspondence | |
| Routine Correspondence | Destroy 4 years from the date of the last entry or last action, unless the correspondence relates to major developments, important local issues or | Routine correspondence and emails<br>General information including invitations, lobbying and promotional material | ACSS Town and Parish Councils document retention schedule and guidance 2025 |

| | | | |
|---|---|---|---|
| | Council decisions not duplicated in minutes, in which case retain for 4 years then preserve. | | |

**Legal and Contracts**

| | | | |
|---|---|---|---|
| Contracts and Tendering – pre contract advice | Destroy 2 years after contract let or not proceeded with | Expressions of interest | |
| Specification and Contract Development – the process involved in the development and specification of a contract | Destroy 6 years after the terms of the contract have expired | Tender specification | |
| Tender Issuing and Return | Destroy 1 year after start of contract | Opening notice Tender envelope | |
| Successful Tender Document | Destroy 6 years after the terms of the contract have expired | Tender documents Quotations | |
| Unsuccessful tender documents | Destroy 1 year after start of contract | Tender documents Quotations | |
| Awarding of contract | Destroy 6 years after the terms of the contract have expired | Signed contract | |
| Contract Management – contract operation and monitoring | Destroy 2 years after the terms of | Service Level Agreements Compliance reports | |

| | | | |
|---|---|---|---|
| | contract have expired | Performance reports | |
| Management and amendment of contract | Destroy 6 years after the terms of the contract have expired | Changes to requirements<br>Variation forms<br>Extension of contract<br>Complaints<br>Disputes on payment | |

**Human Resources**

| | | | |
|---|---|---|---|
| Personnel Administration - summary management systems that allow the monitoring & management of Council Representatives in summary form.<br>Note: The summary information that this record class attempts to capture is:-<br>Name<br>DOB<br>Date of appointment<br>Work history details<br>Position/designation<br>Titles & dates held | Destroy after 7 years from termination | Employment register of both permanent and temporary staff<br>Registers of personnel files<br>Salary master record | |
| The process of administering Council Representatives to ensure that entitlements & obligations are in accordance with | Destroy 6 years from date of last pension payment | Medical clearance<br>Letter of appointment<br>Letter of acceptance<br>Details of assigned duties<br>Probation reports | |

| | | | |
|---|---|---|---|
| agreed employment requirements | | Medical examinations<br>Personal particulars<br>Educational qualifications<br>Declarations of pecuniary interests<br>Employment contracts | |
| Records relating to staff working with children | Destroy 25 years after termination of contract | | |
| All other records | Destroy 6 years after termination of contract | | |
| Council Representative and industrial relations – identifications and development of significant directions concerning industrial matters | Permanent | Generic agreements and awards<br>Negotiations<br>Disputes<br>Claims lodged | |
| Liaison processes of minor and routine industrial matters | Destroy 2 years after administrative use is concluded | Daily industrial relations management | |
| Processes of disciplinary and grievances investigations | Oral Warning – 6 months<br>Written Warning – 1 year<br>Final Warning – 18 months<br>Any warnings involving children need to be placed | Disciplinary | |

| | | | |
|---|---|---|---|
| | permanently on personal file | | |
| Equal Employment Opportunities – the process of investigation and reporting on specific cases to ensure that entitlements and obligations are in accordance with agreed guidelines policies | Destroy 5 years after action completed | | |
| Occupational Health – the process of checking and ensuring the health of staff | Destroy 75 years after D.O.B | Health questionnaire<br>Medical clearance<br>Adjustments to workplace<br>Restrictions<br>Recommendations | |
| Recruitment | Destroy 1 year after recruitment has been finalised | Advertisements<br>Applications<br>Referee reports<br>Interview reports<br>Unsuccessful applicants | |
| Staff Monitoring | | | |
| Performance | Destroy 5 years after action complete | Probation reports<br>Performance plans | |
| Process of monitoring staff leave and attendance | Destroy 2 years after action completed | Sick leave<br>Jury service<br>Study leave<br>Special and personal leave<br>Annual leave | |
| Staff Retention | | | |
| Financial reward | Destroy 7 years after action completed | | |

| | | | |
|---|---|---|---|
| Other strategy | Destroy 3 years after action completed | | |
| Termination – the process of termination of staff through voluntary redundancy, dismissal, and retirement | Destroy 6 years after last payment of pension | Resignation<br>Redundancy<br>Dismissal<br>Death<br>Retirement | |
| Training and Development | | | |
| Routine staff training not occupational health and safety, or children related | Destroy 2 years after action completed | Course individual staff assessment | |
| Training (concerning children) | Destroy 35 years after training completed, or last entry | Course individual staff assessment<br>Training register | |
| Training (occupational health and safety training) | Destroy 50 years after training completed | OH&S training register | |
| Training materials | Individual course assessment records should be destroyed once the training has been renewed – Destroy 1 year after course is superseded. | | |
| Training (proof of completion) | Destroy 7 years after action completed | Certificates<br>Awards<br>Exam results | |
| Volunteers | | | |

| | | | |
|---|---|---|---|
| Personal details | Destroy after volunteering has ceased | | |
| Members | | | |
| Personal details | Destroy after membership has ceased | | |
| Declarations of interest | Destroy after membership has ceased | | |
| Statement of Assurance | Destroy after membership has ceased | | |
| DBS records | Destroy after membership has ceased | | |

**Financial Management**

| Accounts & Audit Reporting | | | |
|---|---|---|---|
| The process that consolidates financial transactions on an annual basis for corporate reporting purposes | Annual audited accounts: retain in Council custody for 7 years, then preserve. Historic ledgers and receipt and payment books: retain for 7 years, then preserve. | Consolidated annual reports<br>Consolidated financial statements<br>Statement of financial position<br>Operating statements<br>General ledger | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| The process that supports and consolidates financial transactions on a periodic (less than annual basis), superseding those from the previous period. Does not include journals and subsidiary | Interim accounts and working papers: retain only where annual accounts do not survive or for administrative/audit need. Otherwise destroy after the last completed audit year or once administrative use is concluded. | Consolidated monthly and quarterly reports<br>Consolidated monthly and quarterly financial statements<br>Working papers for the preparation of the above<br>Monthly accrual statements | ACSS Town and Parish Councils document retention schedule and guidance 2025 |

| | | | |
|---|---|---|---|
| ledgers and cash books | | Cashflow statements<br>Creditor listings and reports<br>Debtor listings and reports | |
| Financial Transactions Management | | | |
| Management of the approvals process for purchase, including investigations | Destroy 7 years after the end of the financial year in which the records were created | Appointments and delegations<br>Audit investigations<br>Arrangements for the provision of goods and/or services | |
| Identification of the receipt, expenditure and write offs of public monies | Cash books, bills, vouchers, bank statements and other subsidiary financial records: retain for 7 years, then destroy.<br>Receipt books, paid invoices, cheques, VAT records, wage books, members' allowance registers, parish hall/recreation ground hiring records and precept books: retain for 7 years, then destroy. | Allowances<br>Work orders<br>Invoices<br>Credit card statements<br>Cash books<br>Receipts<br>Cheque counterfoils<br>Bank statements<br>Vouchers | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Process involving the provision and support for individuals using public transportation | Destroy 6 years after the conclusion of the financial transaction that the record supports | Applications<br>Card issue<br>Rail Warrants | |
| Processes that balance and | Destroy 2 years after its | Reconciliations<br>Summaries of accounts | |

| | | | |
|---|---|---|---|
| reconcile financial accounts | administrative use is concluded | | |
| Taxation Records | Destroy 5 years after the end of the financial year in which the records were created. | Taxation records<br>Motor vehicle logs<br>Fringe benefits tax records<br>Group certificates | |
| Processes involved in the collection of National Insurance Number | Destroy 2 years after the Council Representative ceases engagement or employment | Notification and input records | |
| Payroll Accountable processes relating to payment of Council Representatives | Destroy 7 years after the conclusion of the financial transaction that the record supports | Authority sheets<br>Payroll deduction authorities<br>Payroll disbursement<br>Council Representative pay records<br>Council Representative taxation records | |
| Non-accountable processes relating to payment of Council Representatives | Destroy after administrative use is concluded | Summary Council Representative pay reports | |
| Financial Provisions – Budgets and Estimates | | | |
| The process of finalising local authorities' annual budget | Permanent | Annual budget | |
| The process of developing local authorities' annual budget | Destroy 2 years after annual budget adopted by local authorities | Draft budgets<br>Departmental budgets<br>Draft estimates | |
| The process of reporting which examines the budget in relation | Destroy after next year's annual budget has been adopted by Local Authorities | Quarterly statements | |

| | | | |
|---|---|---|---|
| to actual revenue and expenditure | | | |
| Loans | | | |
| The activity of borrowing money to enable a local authority to perform its functions and exercise its powers | Destroy 7 years after the loan has been repaid | Loan files | |
| Summary management of loans | Permanent | Loans registers | |
| Asset Monitoring and Maintenance | | | |
| Management systems that allow the monitoring and management of assets in summary form | Destroy in 7 years | Subsidiary asset registers | |
| Process of reporting and reviewing assets status | Destroy 2 years after administrative use is concluded | Routine returns and reports on asset status<br>Inventories<br>Stocktaking<br>Acquisition and disposal reports | |
| The process of maintaining assets | Destroy 7 years after last action | Garden maintenance<br>Cleaning<br>Painting | |
| The process of maintaining plant and equipment | Destroy 7 years after disposal of asset | Service records<br>Plant files | |
| Asset Acquisition and disposal – process for assets | Destroy 6 if under £50,000 or 12 years if over £50,000 | Legal documents relating to the purchase/sale<br>Particulars of sale documents<br>Leases | |

| | | | |
|---|---|---|---|
| | | Applications for leases, licences, and rental revision<br>Tender documents<br>Conditions of contracts<br>Certificates of approval | |

**Property and Land Management**

| Property and Land Management | | | |
|---|---|---|---|
| Reports to management on overall property of the local authority | Permanent | Consolidated property and buildings annual reports<br>Summary of leased property<br>Site register<br>Register of leases | |
| Property Development and Renovation | | | |
| The process of managing and undertaking renovations and development of property | Permanent | Project specifications<br>Plans<br>Installation manuals<br>Certificates of approval | |
| The action process involved in the development and renovation of property | 7 years | Work orders<br>Tender contracts<br>Conditions of contracts | |
| Leasing and Occupancy | | | |
| The process of managing leased property | Destroy 15 years after expiry of the lease | Lease agreements<br>Rental expenditure authorities<br>Valuation queries<br>Applications for leases, licences and rental revision | |
| The process of managing the | Destroy 7 years after the conclusion of | Requests for works, cleaning, etc. | |

| | | | |
|---|---|---|---|
| occupancy of property | the transaction that the record supports | | |
| Transport Management | | | |
| The process of acquisition and disposal of vehicles through lease or purchase | Destroy 7 years after the disposal of the vehicle | Leases<br>Contracts<br>Quotes<br>Approvals<br>Fleet authorisation numbers | |
| The process of managing allocation and maintenance of vehicles | Destroy 7 years after the sale or disposal of the vehicle | Approvals as drivers<br>Allocations and authorisations for vehicles<br>Maintenance | |
| The process of recording vehicle usage | Destroy 3 years after the sale or disposal of the vehicle | Vehicle usage reports | |
| The process of recording drivers' usage | Destroy 7 years after closure | Vehicle logbook | |
| Insurance - Policy Management | | | |
| The summary management of insurance arrangements | Insurance register: retain for administrative need.<br>Insurance policies and associated risk assessments should be retained for 40 years from commencement or renewal, then destroyed. | Insurance register | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| The process of insuring local authority officers, property, vehicles and equipment | Insurance policies and associated risk assessments: retain for 40 | Insurance policies<br>Correspondence | ACSS Town and Parish Councils document retention schedule and guidance 2025 |

| | | | |
|---|---|---|---|
| against negligence, loss, or damage | years from commencement or renewal, then destroy. | | |
| The process of renewing insurance policies | Destroy 5 years after the policy has been renewed | Insurance policy<br>Renewal records<br>Correspondence | |
| Insurance - Claims Management | | | |
| The process that records insurance claims against the local authority or local authority officers | Destroy 7 years after closure | Claims records<br>Correspondence | |

## General Public Services

| Health and Safety – Inspections and Assessments | | | |
|---|---|---|---|
| Process of inspecting equipment to ensure it is safe | Destroy 6 years after last use of equipment | Equipment inspection records | |
| Process of carrying out monitoring to ensure that the process is safe | Destroy 3 years from last action | Monitoring results | |
| Process to ensure safe systems of work | Retain until superseded or process ceases for 1 year then can be destroyed | | |
| Process to assess the level of risk | Destroy 3 years from last assessment | Risk assessments | |
| Process that records injuries to adults | Destroy 3 years from closure | Accident books | |
| Process that records injuries to children | Destroy 25 years from closure | Accident books | |

| | | | |
|---|---|---|---|
| Emergency Planning | | | |
| Process to develop the emergency/disaster plan for the local community | Retain for 4 years from the date of the last entry, then preserve if the plan records a significant local emergency, community resilience function or major Council decision. Routine working papers should be retained for administrative need, then destroyed. | Major Incident Plan | ACSS Town and Parish Councils document retention schedule and guidance 2025 |
| Notification | | | |
| The process of issuing notices to citizens with respect to particular responsibilities | Destroy 2 years after the matter is concluded | Fire prevention notices<br>Fire prevention infringement notices<br>Appeals against notices<br>Registration of premises infringement notices | |
| CCTV | | | |
| See CCTV Scheme Retention Policy | | | |

**Miscellaneous**

| | | | |
|---|---|---|---|
| Freedom of Information Requests | Destroy 3 years after closure | | |

| | | | |
|---|---|---|---|
| Press Releases | Destroy 1 year after closure | | |
| Public Consultations | Destroy after 3 years | | |
| Reports, Newsletters | Destroy after 3 years | | |

| | | | |
|---|---|---|---|
| purpose of insuring compliance | Destroy 10 years after the issue of a certificate of final inspection | Certificate of final inspection<br>Building Inspection records<br>Diaries | |
| The process of enforcing building or land regulations | Destroy 3 years | | |

# Redruth Town Council
# Data Subject Rights and Information Access Policy

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## SCOPE

The Data Protection Act 2018 and UK General Data Protection Regulation (**UK GDPR**) collectively known as 'Data Protection Laws', gives individuals ('data subjects') rights in relation to their personal data. This policy explains how Redruth Town Council deals with your requests and objections as a data subject under the UK GDPR when we act as Controller or as a requester under Freedom of Information Act 2000 or Environmental Information Regulations 2004.

## FOIA

### Introduction

As a public authority, Redruth Town Council must comply with the Freedom of Information Act 2000 (FOIA) and relevant ICO Codes of Practice which gives every person a general right of access to 'recorded information' held by it or on its behalf by third-party.

Redruth Town Council is required to respond to written requests for information in accordance with the law. It must also publish its adopted Publication Scheme, which we make available on our website(s) and on our internal policy system.

These processes have been implemented to ensure Redruth Town Council meets its duties under the FOIA Code of Practice.

### Personal Information

Where the requested information constitutes the requester s 'personal information', the request will be rejected and instead handled as a subject access request (later explained by this procedure).

### No Obligation to Create

Redruth Town Council is not under an obligation to create information to respond to a request. The law only applies to information already held by it, or by certain third-parties. The request must be in writing (email is acceptable).

### Requests related to Cornwall Council

Redruth Town Council, predominantly through its Library Service, may hold information on behalf of Cornwall Council. Where Redruth Town Council holds information as Cornwall Council's processor, it must comply with the Agreement with Cornwall Council and must not respond to, disclose, amend, erase, restrict, transfer or otherwise act on any request relating to that information without Cornwall Council's prior written instructions, unless required to do so by law.

Any such request, including a FOIA request, EIR request, subject access request or other data subject rights request, should be logged promptly and referred to Cornwall Council in accordance with the agreed reporting route under the Agreement. Redruth Town Council should provide reasonable assistance to Cornwall Council to enable Cornwall Council to meet its statutory and contractual obligations, including by identifying relevant information, preserving records, providing copies securely, assisting with searches, and applying any required redactions or exemptions where instructed. Staff must ensure that any information held on Cornwall Council's behalf is kept confidential, protected against unauthorised disclosure, and handled consistently with the Agreement and this policy.

**Requests related to CCTV Scheme Participant Councils**

Where a request relates to CCTV Footage or other information processed under the Redruth Town Council CCTV Scheme on behalf of another Participant Council, Redruth Town Council must handle the request in accordance with the Scheme Code of Practice and Scheme Policies.

**Request Handling Process**

Upon receipt, Redruth Town Council will log the request and assess whether the information is already made available to the requester within the Publication Scheme or otherwise available. If so, the requester will be directed to the public source as soon as possible. Where information will shortly be published by Redruth Town Council, for example through its publication scheme, and it is reasonable to withhold the information until that later date then we may consider refusing (or deferring) disclosure under Section 22 of the FOIA.

Where information is not already (or soon likely to be) readily available, Redruth Town Council will acknowledge receipt of the request and inform you of the expected date of response (including any application of the public interest test extension discussed below).

Redruth Town Council must respond to requests within 20 working days of the date of receipt of the Request unless a public interest test extension of no more than an additional 20 working days applies.

Redruth Town Council's response will:

- Confirm whether information is held by the Council. Where Redruth Town Council relies on certain exemptions, it may refuse to confirm or deny whether it holds the requested information in question where confirming or denying would, in itself, reveal information that is exempted from disclosure;
- as far as reasonably practicable, provide the requester with the requested information (subject to exemptions) in their preferred format.

**Exemptions**

Exemptions to disclosure under FOIA can be found here List of exemptions | ICO.

If the information falls within an exemption under FOIA, Redruth Town Council will determine whether:

- The information can be disclosed in any event (for example, because the authority chooses not to apply the exemption, or in the case of confidential information from third parties, consent to disclose has been obtained from those third parties);
- The information can be edited or redacted before publication and the remainder disclosed.
- In the case of any information the authority wishes to withhold and which engages a qualified exemption, the public interest in maintaining the exemption outweighs the public interest in disclosure.

If information requested is withheld, Redruth Town Council will issue a refusal notice meeting the requirements of section 17 of FOIA. This will include:

- The information exempted from disclosure.
- Which exemption(s) apply.
- If the exemption is qualified, the reasons why the public interest test favours withholding the information.
- The procedure for appealing the refusal, including whether the Redruth Town Council has an internal review procedure and the requester's right to complain to the Information Commissioner if they are dissatisfied with the outcome of the internal review.

**Vexatious or repeated requests**

Public authorities are not required to comply with vexatious requests (section 14 , FOIA). It is the request, not the applicant, that must be vexatious. Examples of vexatious requests could include requests that are:

- Frivolous.
- Aimed at disrupting the work of an authority.
- Aimed at causing distress to individuals.

When responding to a vexatious applicant, Redruth Town Council is not required to explain why the request is vexatious (although we may wish to do so as part of our advice and assistance to the requester).

Similarly, Redruth Town Council is not obliged to comply repeatedly to the same or a substantially similar request from the same applicant until a reasonable period has passed.

**Costs and Cost Limit**

Redruth Town Council will not charge you for your actioning your request. We are however permitted to charge for disbursements in accordance with our internal Charging Policy.

Redruth Town Council is not obligated to respond to a request that exceeds the statutory costs limit (being £450 for Redruth Town Council) in respect of each individual request. The cost of an individual officer's time is £25 per hour. It follows the attached ICO guidance when calculating this fee: Requests where the cost of compliance exceeds the appropriate limit (section 12) | ICO. Where the Data Protection Officer of Redruth Town Council reasonably believes that the costs limit will be exceeded, it is permitted to decline the request, ask you to limit your request or provide the information on receipt of the calculates fee. The costs of answering one or more request may be aggregated in limited circumstances.

**Advice and Assistance**

Redruth Town Council will offer advice and assistance where:

- we require further information from you to identify and locate the information requested. (The 20 working day time limit will not start until the request has been clarified.)
- we do not hold the requested information but can direct the requester to the appropriate authority.
- compliance with the request would exceed the cost limit but the applicant may be able to refine the request to bring it within the cost limit. (The 20 working-day time limit will continue to run.)

**EIR**

As a public authority, Redruth Town Council must comply with the Environmental Information Regulations (2004) (**EIR**) and relevant ICO Codes of Practice, which give any person a general right of access to “environmental information” held by it or on its behalf by a third party.

Environmental information is defined broadly in regulation 2(1) EIR. It includes information in any form that is on the state of environmental elements, the factors affecting them, and the measures or activities affecting or likely to affect those elements or factors, including administrative measures. Information may fall within

this definition even where it is not inherently environmental, provided it relates to a measure or activity that would, or would be likely to, affect the environment. Certain information that appears environmental may fall outside the definition.

Usually, it will be obvious what information is environmental (for example, information about land development, pollution levels, energy production, and waste management). However, some information may seem like environmental information, but it does not fall within the definition of 'environmental information' for the purposes of the Act. More information on what qualifies as 'environmental information' can be found here. If you are uncertain whether the information you seek qualifies as environmental information, you may ask a member of our team for further assistance.

**Personal Information**

Where the requested information constitutes the requester's personal information, the request will be refused (regulation 5(3) EIR) and instead handled as a subject access request, as explained later in this procedure.

**No Obligation to Create Information**

As with FOIA requests, Redruth Town Council are under no obligation to create information. The law only applies to information already held.

**Format of Request**

Redruth Town Council is required to respond to verbal or written EIR requests for environmental information.

**Request Handling Process**

Upon receipt, Redruth Town Council will log the request and assess whether the requested environmental information is already publicly available. If so, the requester will be directed to the public source as soon as possible.

Where the information is planned for publication at a future date, the Council may consider applying the exception under regulation 12(4)(d) EIR (material still in the course of completion or incomplete data).

Where the information is not already (or soon to be) publicly available, the Council will acknowledge receipt of the request and confirm the expected date of response, including whether any extension for complex or voluminous requests applies.

Redruth Town Council must normally respond within 20 working days, but where the request is complex and voluminous, the EIR permits an extension to 40 working days.

Redruth Town Council's response will:

- Confirm whether the environmental information is held (unless exempt).
- Provide the information in the requester's preferred format, as far as reasonably practicable.

**Presumption in favour of disclosure**

The EIR require Redruth Town Council to apply a presumption in favour of disclosure of environmental information requested of it. We may, however, refuse disclosure where an exception under EIR applies and, in all the circumstances of the case, the public interest in maintaining the exception outweighs the public interest in disclosing the information.

**Exceptions**

Where an EIR exception applies, Redruth Town Council will consider whether disclosure would adversely affect the relevant protected interest. The Council must be satisfied that the envisaged harm is more likely than not to occur and that there is a causal link between disclosure and the anticipated adverse effect. All exceptions, other than those relating to personal data, are subject to the public interest test, and the Council will apply the statutory presumption in favour of disclosure.

Certain exceptions cannot be relied upon where the requested information relates to emissions into the environment (regulation 12(9) EIR).

If the information falls within an exception under the EIR, Redruth Town Council will consider:

- Whether information can nevertheless be disclosed (for example, because we choose not to apply the exception, or because consent has been obtained from third parties, where applicable).
- Whether the information can be edited or redacted with the remainder disclosed.
- Most EIR exceptions are subject to the public interest test, meaning the Council must determine whether the public interest in maintaining the exception outweighs the public interest in disclosure.

If information is withheld, Redruth Town Council will issue a refusal notice that:

- Identifies the information being withheld.
- Confirms which EIR exception(s) apply.
- Explains why the public interest favours withholding the information.
- Sets out the appeal process, including internal review rights and the requester's right to complain to the Information Commissioner.

**Manifestly Unreasonable Requests**

Redruth Town Council is not required to comply with manifestly unreasonable requests (regulation 12(4)(b) EIR). This may include requests that would impose unreasonable burdens, including excessive cost or resource impact, or those that appear to be harassing or vexatious in nature.

When assessing whether a request is manifestly unreasonable, the Council will take into account recognised factors including the burden of compliance, the value or purpose of the request, the context and history of contact, and any evidence of harassment or improper motive. These factors derive from established case law applicable to this exception. Cost may form part of this assessment (although there is no statutory costs limit to an EIR request).

Where the Council refuses a request on this ground, it will provide reasonable advice and assistance to enable the requester to refine the scope of their request.

The Council may explain why a request is considered manifestly unreasonable as part of its duty to provide advice and assistance.

**Charges**

The Council may levy a reasonable charge for making environmental information available (regulation 8 EIR). Any such charge will be limited to the actual costs of supplying the information, which may include staff time and attributable overheads for locating, retrieving, extracting and preparing the information for disclosure, together with reasonable disbursements. Charges will not exceed the cost of supply. A schedule of applicable charges will be published by Redruth Town Council.

No charge will be made for allowing inspection of public registers or for in-person examination of the information.

**Advice and Assistance**

Redruth Town Council will offer reasonable advice and assistance where:

- We require further information from the requester to identify and locate the environmental information. (A new 20 working day period begins upon receipt of information.)
- We do not hold the information but can direct the requester to another authority that may hold it.

## SUBJECT RIGHTS REQUESTS

You can make Data Subject Requests in relation to the following rights:

1. Access to your personal data;
2. Correct your personal data;
3. Erase your personal data;
4. Restrict personal data processing about you;
5. Receive a copy of certain personal data or transfer that personal data to another controller, also known as the data portability right;
6. Object to personal data processing; and
7. To not be subject to automated decision-making, including profiling, in certain circumstances.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

Redruth Town Council is committed to operating openly, transparently, and to meeting all reasonable lawful requests for information that are not subject to specific exemption in the Act.

### Identify verification

If you make a request, we will first check that we have enough information to confirm your identity. We will ask you to provide any evidence we reasonably need to confirm your identity.

If you are making a request on behalf of another person, we require proof of your authority to act on behalf of the data subject.

## The cost of a request

We must generally respond to a request for free. However, the law permits us to charge a fee when requests are manifestly unfounded or excessive, because of their repetitive character or when the request relates to large amounts of data.

## Data subject request refusal

We may refuse to respond to your request for the following reasons:

(a) You fail to present sufficient proof of authority or identity to make the request;

(b) The law prevents us from responding to the request;

(c) We demonstrate that the request is manifestly unfounded or excessive, in particular because of its repetitive character; or

(d) We do not hold any personal data related to you or any data held does not directly or indirectly identify you.

Where we refuse to respond to your request we will explain the reason for such refusal.

## 1. SUBJECT ACCESS REQUESTS

### Making a Subject Access Request (SAR)

We recognise that you can make SARs verbally or in writing, including via social media. In the first instance, we request that all applicants contact us via townclerk@redruth-tc.gov.uk

### Our acknowledgment of your SAR request

We will contact you in writing to inform you that we have received your request and that you should expect to receive a response within one month.

### How we process SARs

We will check that we have enough information from you to process the request. If we need more information from you to assist us in our search we will promptly request this from you. This will have the effect of ‘stopping the clock’ on the request until such information is provided.

We will make reasonable efforts to find and retrieve the requested information. However, we are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

## Data relating to third-parties within a SAR

We are not required to disclose information relating to third parties, unless they have provided their consent or it is reasonable to do so without their consent. In some cases, it may not be suitable to obtain the third-party's consent (for example where harm may be caused by obtaining such consent). We may need to seek legal advice on application of this exemption.

Where it is not suitable to provide you with such third-party information, we shall take steps to redact or omit such information from our SAR response.

The right of access does not automatically grant a right to documents. If necessary, we may summarise the information (rather than provide a full copy of the document).

## Responding to your SAR

Once we have confirmed identification, resolved any queries around the applicant's request, and gathered the relevant information, we will issue our response to using the original method of communication. For example, if you email us with your request, we will email you with our response.

Any postal SAR will receive our response by recorded delivery in an envelope or package marked 'Private and Confidential' and 'Addressee Only'.

## Timescale for SAR response

The law gives us one month from the date of receipt of your SAR to respond.

Where your request is complex or you have made a number of requests to exercise your data rights, we may require more time to provide you with a substantive response and the law permits us a further two months to respond to you in such circumstances. If an extension is required, we will write to you within the initial one-month timeframe to inform you of this extension (including our reasons for the same and an anticipated response date).

## Grounds for not complying with a SAR

The UK GDPR contains a number of exemptions to our duty to disclose personal data, and we may seek legal advice if we believe one or more of these exemptions may apply to the request. We can also refuse to comply with a SAR if it is:

- manifestly unfounded; or
- manifestly excessive.

Details of these exemptions can be found on the Information Commissioner's Office (ICO) website.

## 2. RIGHT TO RECTIFICATION

If you identify an error in the information we hold about you, please notify us as soon as possible.

If we agree that the information is inaccurate we will take all reasonable steps to correct the information or if relevant and practically possible, remove the inaccurate information by deletion or destruction. We will inform of when such rectification has taken place you using your original method of communication

We will also take steps to identify each third-party recipient of the personal data that is the subject of the rectification and communicate the rectification of the personal data to each recipient unless such communication or identification is impossible or involves disproportionate effort.

## 3. RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

This right applies in the following circumstances:

(a) The personal data is no longer necessary in relation to the purpose for which it was originally collected;

(b) The processing was based on consent, and you have now withdrawn your consent;

(c) you object to processing and we do not have an overriding legitimate interest as Data Controller;

(d) The data was being unlawfully processed; and

(e) The data must be erased to comply with a legal obligation.

If we determine that we must erase your data in response to the request, we will take reasonable steps to seek erasure from any third-party data recipients, unless such action is impossible or involves disproportionate effort.

We may also refuse to respond to an erasure request if we process personal data that is necessary for:

(a) Exercising the right of freedom of expression and information.

(b) Complying with a legal obligation.

(c) The performance of a task carried out in the public interest.

(d) Exercising our official authority.

(e) Public health reasons consistent with the exceptions for processing sensitive personal data such as health information.

(f) Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, if the erasure is likely to render impossible or seriously impair the processing objectives.

(g) The establishment, exercise, or defence of legal claims.

## 4. RIGHT TO RESTRICT PROCESSING

You have the right, in certain circumstances, to request that we restrict the processing of your personal data.

Examples of restrictions include:

(a) You contest the accuracy of the personal data we hold. We must restrict processing the contested data until we can verify its accuracy.

(b) The processing is unlawful. Instead of requesting erasure of the data, you can request that we restrict use of the unlawfully processed personal data.

(c) We no longer need to process the personal data but you need the personal data for the establishment, exercise, or defence of legal claims.

(d) you object to processing, including profiling, for:

a. purposes that we consider necessary to perform a task in the public interest; or

b. purposes that we consider necessary for our or a third party's legitimate interests.

Where processing is restricted, we may retain a right to process your personal data in certain circumstances including where we have your consent, where we must establish, exercise, or defend legal claims, where we need to protect another person and for reasons of public interest.

## 5. RIGHT TO DATA PORTABILITY

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one service provider to another in a safe and secure way in a common data format, for example, Excel or CSV file. We will make reasonable efforts to transmit the personal data using a method you have request.

The right applies in the following circumstances:

(a) When the personal data was provided to the controller directly by you;

(b) Where the processing is based on consent or performance of a contract;

(c) When processing is carried out by automated means.

## 6. RIGHT TO OBJECT

You may object to processing where processing is based on legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and for the purposes of scientific/historical research and statistics.

We can refuse to grant an objection when:

(a) You object to processing for scientific or historical research purposes or statistical purposes and we can demonstrate that the processing is necessary for us to perform a task in the public interest.

(b) You object to processing, including profiling, based on processing for a task in the public interest or in our (or a third-party's) legitimate interest and we can demonstrate:

   a. a compelling legitimate ground for processing the personal data that overrides your interests; or

   b. that we need to process the personal data to establish, exercise, or defend legal claims.

## 7. RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

This right provides you with the right to be safeguarded from potentially adverse decisions made without human intervention.

The right applies when a decision is based on automated processing and produces legal/significant effects on you. It does not apply if the decision:

(a) is necessary for entering into or performance of a contract;

(b) is authorised by law;

(c) is based on explicit consent; or

(d) does not have a legal/significant effect on the data subject

## 8. RIGHT TO WITHDRAW CONSENT

To withdraw your consent, please contact the Data Protection Officer, Charlotte Williams, by emailing townclerk@redruth-tc.gov.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your

information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## RE-USE OF PUBLIC SECTOR INFORMATION

Redruth Town Council is a public sector body for the purpose of the Re-use of Public Sector Information Regulation 2015. These Regulations govern how information produced as part of the Council's public task may be re-used by individuals, businesses or other organisations. RPSI Concerns the terms on which information may be re-used; it does not provide a right of access to information. Access is dealt with under UK GDPR/Data Protection Act 2018, Freedom of Information Act 2000, the Environmental Information Regulations 2004 and other relevant access legislation.

To make a request for re-use of public information or more information in relation to our Information Assets, please contact the Town Clerk by email townclerk@redruth-tc.gov.uk. Permitted charges may apply.

## IF WE CANNOT PROCESS YOUR REQUEST

If we believe your request cannot be actioned, we will inform you of the reason(s) for not acting and inform you of your right to lodge a complaint with the supervisory authority and seeking a judicial remedy.

## OUR DATA PROTECTION COMPLAINTS PROCEDURE

Individuals have the right to raise a data protection complaint directly with Redruth Town Council if they consider that we have infringed data protection law in the way we have handled their personal data. This includes complaints about how we have collected, used, disclosed, retained or protected personal data, or how we have responded to a data subject rights request.

A complaint may be made in writing to the Town Clerk or Deputy Town Clerk, including by email to townclerk@redruth-tc.gov.uk. We will also recognise data protection complaints received through other communication channels where it is reasonably clear that the individual is unhappy with how we have handled their personal data. If we are unsure whether a communication is intended to be a data protection complaint, we may ask the individual to clarify this.

We will acknowledge receipt of a data protection complaint within 30 days of receiving it. Where appropriate, we may ask for further information to understand the complaint, verify identity or confirm authority where a complaint is made on behalf of another individual.

We will take appropriate steps to investigate and respond to the complaint without undue delay. This may include making relevant internal enquiries, reviewing records,

considering whether any remedial action is required and keeping the complainant informed of progress where the matter cannot be concluded promptly.

Once our investigation is complete, we will inform the complainant of the outcome without undue delay. Our response will explain, where appropriate, whether the complaint has been upheld, partly upheld or not upheld, any action we have taken or propose to take, and the complainant's right to complain to the Information Commissioner's Office if they remain dissatisfied.

If you remain dissatisfied after we have considered your complaint, you have the right to report your concern to the Information Commissioner's Office (ICO). You can do this by visiting their website (https://ico.org.uk/) or by calling them on 0303 123 1113

# Redruth Town Council
# Member, Officer, Volunteer and Contractor Privacy Notice

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## 1. INTRODUCTION AND IMPORTANT INFORMATION

1.1 Redruth Town Council ("we", "us" or "our") are committed to protecting and respecting your personal data and privacy. This privacy notice relates to how we use and collect personal data about you during and after your working relationship with us.

1.2 Whenever you provide personal data, we are legally obliged to use your information in line with all applicable laws concerning the protection of such information; including but not limited to the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR), described in this policy as the "Data Protection Laws".

1.3 For the purpose of the Data Protection Laws, Redruth Town Council is the data controller. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

1.4 This privacy notice applies to:

1.4.1 current and former employees, apprentices, workers and contractors (of the Council excluding event traders, contributors and performers who are covered by the Redruth Town Council Privacy Notice);

1.4.2 Volunteers including library volunteers, operational volunteers (such as de cluttering volunteers) and those recruited via third-party charities and organisations but excluding Youth Council volunteers and library Summer Reading Challenge volunteers; and

1.4.3 members/elected representatives, including Councillors, acting in their Council capacity.

together "**Council Representatives**".

We may amend or update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

## 2. DATA PROTECTION PRINCIPLES

2.1 We will comply with data protection law. This says that the personal information we hold about you must be:

2.1.1 Used lawfully, fairly and in a transparent way;

2.1.2 Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;

2.1.3 Relevant to the purposes we have told you about and limited only to those purposes;

2.1.4 Accurate and kept up to date;

2.1.5 Kept only as long as necessary for the purposes we have told you about;

2.1.6 Kept securely;

## 3. THE DATA WE COLLECT ABOUT YOU

3.1 Personal data, or personal information, means any information about an individual from which that person can be identified (for example, your name, email address, unique identification number etc.). It does not include data where the identity has been removed (anonymous data or pseudonymised data).

3.2 Typically, the personal data we collect and process will include Identity, Contact, Employment, Financial, Profile, Technical, and CCTV Data:

3.2.1 **Identity Data** includes first name, last name, title or other identifier (such as job title), marital status, dependents, date of birth, gender and images.

3.2.2 **Contact Data** includes billing addresses, email addresses, telephone numbers and emergency contact information.

3.2.3 **Employment Data** includes employment history, salary, working hours, annual leave, pension and benefits information, start and leaving date of employment, location of workplace, CV and cover letters, right to work documentation, employment references, training records, professional memberships, performance information, disciplinary and grievance information.

3.2.4 **Financial Data** includes bank account details, national insurance number, payroll records, compensation history, and tax status information.

3.2.5 **Profile Data** includes your username and password, interests, preferences, feedback and survey responses.

3.2.6 **Technical Data** includes information about your use of our information and communications systems.

3.2.7 **CCTV Data** includes data (including but not limited to images, video and sound) gathered by Closed Circuit Television, Automatic Number Plate Recognition and other surveillance technologies installed at our property.

3.2.8 **Member Data** includes information relating to your role as an elected representative, including declarations of interest, attendance records, voting history, register of gifts and hospitality, committee membership, published contact information, correspondence generated in the course of Council business, and any biographical information you choose to provide for publication.

3.2.9 **Volunteer Data** includes information relating to your volunteering role, including application details, skill or experience information relevant to

your placement, training records, schedules and activity logs, safeguarding information where applicable, and any correspondence relating to the administration or supervision of your volunteering activities.

3.3 In certain circumstances, we may collect Special Categories of Personal Data about you, more sensitive personal data which require a higher level of protection, such as:

3.3.1 Information about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions;

3.3.2 Trade union membership;

3.3.3 Information about your health, including any medical condition and sickness records;

3.3.4 Genetic information and biometric data; and

3.3.5 Information about criminal convictions and offences.

## 4. HOW IS YOUR PERSONAL DATA COLLECTED?

4.1 We use different methods to collect data from and about you including:

4.1.1 **Direct interactions**, including when you submit application forms or corresponding with us by post, phone, messaging service, email or otherwise. We may also collect additional personal information throughout the course of your employment.

4.1.2 **Third parties or publicly available sources**, including contractors engaged by Redruth Town Council, Cornwall Council (where applicable such as the Library), former employers, employment agencies, credit reference agencies, background check agencies and social media platforms.

4.1.3 **Data generated by monitoring or security tools** including CCTV, IT logs or security system outputs.

## 5. IF YOU FAIL TO PROVIDE PERSONAL DATA

5.1 Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our employees people).

In this case, we may have to cancel all or part of a service you have with us, but we will notify you if this is the case.

## 6. LAWFUL BASIS FOR PROCESSING

6.1 We will only process your personal data where a legal ground for processing has been identified (also commonly known as 'valid lawful basis'). This could be:

6.1.1 Where you have given your consent to the processing (Article 6(1)(a) of the UK GDPR – Consent)

6.1.2 Where it is necessary for the performance of a contract with you (Article 6(1)(b) of the UK GDPR – Contractual)

6.1.3 Where we need to comply with our legal obligations (Article 6(1)(c) of the UK GDPR – Legal Obligation)

6.1.4 Where it is necessary for our legitimate interests pursued or the legitimate interest of others, and your interests and fundamental rights do not override those interests (Article 6(1)(f) of the UK GDPR – Legitimate Interest)

6.2 In limited circumstances, we rely on your consent for processing, such as when we process your data outside our contractual obligations or when we handle Special Category Personal Data for any non-employment related purpose. We may process your personal data without your knowledge or consent where this is required or permitted by law. If we collect consent, we will inform you how we do so, the circumstances when this may be required and how you are able to exercise your right to withdraw consent.

6.3 In limited circumstances, we may also use your personal data in the following ways:

1. For the protection of you or others' interests (Article 6(1)(d) of the UK GDPR – Vital Interests); or
2. For the performance of a task carried out in the public interest or for official purposes (Article 6(1)(e) of the UK GDPR – Public Task).

## 7. HOW YOUR DATA WILL BE USED

7.1 We have set out below in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data, where more than one ground has been set out in the table below.

| **All individuals covered by this policy** | | |
|---|---|---|
| **Purpose/Activity** | **Type of data** | **Lawful basis for processing including basis of legitimate interest** |
| Training and Development | As applicable to the training provided | Public task (to ensure Council Representatives are adequately trained to discharge statutory and organisational functions)<br>Legal obligation (where training is required by law, such as health and safety or safeguarding). |
| Wellbeing, Pastoral or Occupational Support. | Identity<br>Contact<br>Employment<br>Special Category Data (Health), where support relates to health or adjustments<br>Volunteer Data<br>Member Data | Public task (to support the effective functioning of Council Representatives in delivering statutory duties).<br>Legal obligation (health and safety, duty of care).<br>Special category condition: Schedule 1 DPA 2018 (employment, social protection, or health and safety). |
| Systems access rights and usage, including systems access management, password administration, and account administration | Identity, Contact, Technical | Public task (to operate Council systems required for the performance of official functions)<br>Legal obligation (information security) |
| Safeguarding Requirements such as Disclosure and Barring Service (DBS) checks | Identity, Contact, Special Category Data (Criminal offence data) | Necessary to comply with a legal obligation (safeguarding)<br>Special category/Criminal offence condition: Schedule 1 DPA 2018 (employment, social protection, or safeguarding) or explicit consent where required. |

| | | |
|---|---|---|
| To facilitate business management and administration including:<br>Business and workforce planning<br>Accounting and auditing<br>Ensuring information and network security<br>Internal governance, audit and oversight<br>Emergency planning<br>Union relations (where applicable) | Identity<br>Contact<br>Employment<br>Financial<br>Profile<br>Technical<br>CCTV<br>Volunteer Data<br>Special Category Data (Trade Union) | Public task (necessary to support efficient and lawful operation of Council functions)<br>Necessary to comply with a legal obligation (legal, regulatory, tax, accounting and reporting)<br>Necessary for our legitimate interests (to run and protect our business) |
| To record incidents and accidents occurring at Council premises, administer related insurances, and meeting other health and safety obligations. | Identity<br>Contact<br>CCTV<br>Special Category Data (Health)<br>Volunteer Data | Necessary to comply with a legal obligation (health and safety)<br>Necessary for our legitimate interests (to ensure our property is secure and fit for use and to ensure the wellbeing of employees, workers and contractors)<br>Public task (to maintain a safe environment for Council Representatives and visitors) |
| Management of departing personnel. | As applicable | Public task (to administer the conclusion of official or working relationships and ensure ongoing security of the Council and its assets/data)<br>Legal obligation (where statutory retention or reporting duties apply) |
| Recognition, Rewards and Engagement | Identity<br>Contact<br>Employment Data<br>Volunteers Data | Legitimate interests (to support morale, engagement and organisational culture). |

| | | |
|---|---|---|
| | Member Data | |
| Images and video taken of Council activities and Events used for promotional purposes where you may be present (including Social media and our Websites). | Images | Legitimate interests (to promote the Council and its activities). You may object to this processing activity at any time by informing your line manager. |
| **Employees and Workers** | | |
| To register you as a new employee, worker or contractors and set up your account profile | Identity<br>Contact<br>Employment<br>Financial<br>Profile<br>Special Category Data (Health)<br>Volunteer Data | Performance of a contract with you |
| To facilitate recruitment and employment or engagement:<br>Determining the terms of employment<br>Checking your right to work in the UK<br>Making salary payments to you and confer benefits in connection to your employment<br>Enrolling you in a pension arrangement<br>Providing workplace adjustments<br>Conducting performance reviews and determining performance requirements<br>Gathering evidence for complaint, grievance or disciplinary procedures | Identity<br>Contact<br>Employment<br>Financial<br>Profile<br>Special Category Data (Health, Biometric)<br>Volunteer Data | Performance of a contract with you<br>Necessary to comply with a legal obligation<br>Necessary for our legitimate interests (to recruit a candidate best suited for the position, to provide equal opportunities and to study employee satisfaction and retention) |

| | | |
|---|---|---|
| Asking you to take a survey | | |
| Statutory reporting and administration of statutory schemes. | Identity<br>Contact<br>Employment<br>Financial<br>Special Category Data (where required by law) | Legal obligation (statutory reporting, taxation, pension administration, workforce reporting). |
| **Volunteers** | | |
| To register you as a volunteer and administer your volunteering relationship with us. | Identity<br>Contact<br>Profile<br>Special Category Data (Health) | Public task (where volunteering activity supports delivery of statutory or public functions)<br><br>Legal obligation (where required for safeguarding, health and safety, or statutory reporting) |
| To manage volunteering activity, including:<br>Allocating tasks, suitability assessments<br>Coordinating schedules<br>Providing training<br>Monitoring participation<br>Implementing safeguarding measures | Identity<br>Contact<br>Profile<br>Technical<br>Special Category Data (Health) | Public task (to coordinate volunteer activities that support Council functions)<br><br>Legal obligation (health and safety, safeguarding where applicable) |
| To maintain security and protect our premises, systems and people. | Identity<br>Contact<br>CCTV<br>Technical | Public task (to maintain secure operations)<br>Legal obligation (health and safety) |
| **Elected Representatives** | | |
| Election-related processing | Identity<br>Contact<br>Member Data<br>Special Category Data (Political opinions) where required for nomination or | Public task (to administer elections and support the democratic process).<br><br>Legal obligation (electoral legislation).<br><br>Special category condition: |

| | | |
|---|---|---|
| | statutory electoral purposes. | Schedule 1 DPA 2018 (substantial public interest – democratic engagement). |
| To register you as an elected representative and enable you to carry out your official functions, including matters relating to Standards, Ethical Management and Code of Conduct Management. | Identity<br>Contact<br>Profile<br>Member Data | Public task (to support you in performing your statutory and democratic functions) |
| To administer allowances, expenses and financial entitlements connected with your elected role, if applicable. | Identity<br>Contact<br>Financial<br>Member Data | Legal obligation (statutory duties relating to payments, taxation and transparency)<br>Public task |
| To publish information required by law or good governance practice, including declarations of interests, attendance records, and contact information. | Identity<br>Contact<br>Profile<br>Member Data | Legal obligation (publication duties under relevant local government legislation)<br>Public task |
| To record attendance at meetings, minutes, decisions taken, and other democratic processes. | Identity<br>Contact<br>Profile<br>CCTV (where meetings are recorded)<br>Member Data | Public task (to support democratic accountability and transparency)<br><br>Legitimate interests (to maintain an accurate record of proceedings) |
| To maintain security and protect our premises, systems and people. | Identity<br>Contact<br>CCTV<br>Technical<br>Member Data | Legitimate interests (to ensure the security of the Council and its members)<br><br>Legal obligation (health and safety) |
| **Contractors** | | |
| To manage contractor access to Council | Identity<br>Contact<br>Employment | Public task (to maintain secure and effective operations) |

| | | |
|---|---|---|
| premises, systems and information | (where applicable to the engagement)<br>Financial<br>Technical (where systems access is required) | Legal obligation (health and safety and information security)<br><br>Legitimate interests (to protect Council assets, staff and visitors) |
| To register you as a contractor and administer your working relationship with the Council | Identity<br>Contact<br>Employment (where applicable to the engagement)<br>Financial<br>Technical (where systems access is required) | Performance of a contract with you<br><br>Legal obligation (including taxation, financial transparency, and procurement compliance) |
| To ensure health and safety compliance during your provision of services | Identity<br>Contact<br>CCTV<br>Special Category Data (Health) where required for risk assessments or incident reporting | Legal obligation (health and safety)<br><br>Special category condition: Schedule 1 DPA 2018 (health and safety or statutory purposes) |
| To facilitate procurement, contract monitoring, audit, and financial administration | Identity<br>Contact<br>Financial<br>Technical (where relevant to contract performance) | Legal obligation (financial reporting, audit, procurement regulation)<br><br>Public task (delivery of statutory functions reliant on contracted services)<br><br>Legitimate interests (to ensure value for money and oversight of contractor performance) |
| To respond to incidents, complaints or disputes involving contractors | Identity<br>Contact<br>CCTV<br>Employment | Public task (investigation and resolution of matters affecting Council functions) |

| | | |
|---|---|---|
| | (where relevant) Special Category Data (where incident circumstances require it) | Legal obligation (regulatory or safety requirements)<br><br>Legitimate interests (to protect the Council's legal and operational interests)<br><br>Special category condition: Schedule 1 DPA 2018 (legal claims or regulatory requirements) |

## 8. MONITORING

We may monitor the use of our premises, information systems and equipment where this is reasonable, proportionate and necessary for a defined purpose. Monitoring may include review of IT system logs, access records, security alerts, email metadata, CCTV footage and other audit trails generated through your use of Council systems. Activities related to limited monitoring of personal devices can be found under our BYOD Policy.

All Council Representatives are informed that monitoring of systems and communications may take place. Monitoring is carried out in accordance with the Data Protection Act 2018 and the UK GDPR, and only for purposes such as ensuring the security of our networks and data, detecting unauthorised use, complying with legal or regulatory obligations, safeguarding, and preventing or detecting wrongdoing.

We do not use monitoring for continuous assessment of performance unless you have been expressly informed that this will occur and the monitoring is justified and proportionate. Any monitoring undertaken will be limited to what is necessary to achieve the stated purpose and will be subject to appropriate safeguards.

## 9. AUTOMATED DECISION MAKING

9.1 Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following ways:

9.1.1 Where we have notified you of the decision and given you 21 days to request for a reconsideration;

9.1.2 Where it is necessary to perform a contract with you;

9.1.3 Where it is authorised by law;

9.1.4 In limited circumstances, where you have given explicit written consent.

9.2 You will not be subject to a decision that will have a significant impact on you based solely on automated decision-making, unless we have a valid lawful basis for doing so and we have notified you.

9.3 We do not envisage that any decisions made about you will be made using automated means. Should this position change, we will notify you in writing and ensure that appropriate measures are in place to safeguard your rights.

## 10. THIRD PARTIES AND SHARING INFORMATION

10.1 We may share your data with third parties, including third-party services where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

10.2 All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions. We never sell your data to third parties or allow third parties to contact you without your permission.

10.3 Please see below list which sets out the categories of third parties which may receive your personal data.

| **THIRD-PARTIES WHO MAY RECEIVE YOUR PERSONAL DATA** |
|---|
| Cornwall Council and their systems (where applicable such as Library Staff and Volunteers) |
| Members, as permitted by the Redruth Town Council Information Access Protocol |
| IT support services |
| Email provider |
| Website provider |
| Software providers |
| Feedback aggregators and collectors |
| Banks |
| Online payment providers |
| Payroll provider |
| Pension administrator |

| |
|---|
| Professional advisors (accountants, solicitors, insurers) |
| DBS Check providers |
| Secure document disposal service |
| Couriers |
| Training providers |
| Recruitment agencies, professional bodies and JobCentre Online |
| Marketing agencies |
| Fraud prevention agencies |
| Credit reference agencies |
| Law enforcement bodies (where necessary) |

10.4 We may need to disclose your personal information with any competent law enforcement body, regulator, government agency or court to comply with our legal obligations (for instance, HMRC).

10.5 In the event that we sell or buy any business or assets, we may disclose your personal data we hold to the prospective seller or buyer of such business or assets. Such disclosure will be subject to the seller or buyer's processing of your personal data on terms equal to the protections afforded to you by this policy.

## 11. INTERNATIONAL TRANSFERS

11.1 We store your personal data in the UK. However, some of our external third-party service providers are based outside the UK, including the European Economic Area. Where your personal data is transferred outside the UK, we ensure a similar degree of protection is afforded to it by implementing at least one of the following safeguards. We will either:

11.1.1 Transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the Information Commissioner; or

11.1.2 Put in place an appropriate data transfer mechanism, such as the Standard Contractual Clauses (SCCs) or the International Data Transfers Agreement (IDTA) approved by the UK regulatory authority, the Information Commissioner's Office.

11.2 Please contact us for further information on the specific transfer mechanisms we rely on when sending personal data outside the UK.

## 12. DATA SECURITY

12.1 We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those Council Representatives and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

12.2 We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

## 13. DATA RETENTION

13.1 We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a disciplinary procedure or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

13.2 To determine the appropriate retention period for personal data, we consider:

13.2.1 the amount, nature and sensitivity of the personal data;

13.2.2 the potential risk of harm from unauthorised use or disclosure of your personal data;

13.2.3 the purposes for which we process your personal data and whether we can achieve those purposes through other means; and

13.2.4 The applicable legal, regulatory, tax, accounting or other requirements.

13.3 In some circumstances, we may anonymise your personal data (so that it can no longer be associated with you), in which case we may use this information indefinitely without further notice to you.

13.4 For more information on our standard Retention Periods. Please visit our Data Retention Policy.

13.5 Once you are no longer a Council Representative, we will securely destroy or erase your personal information in accordance with our Data Retention Policy. For further details on our retention periods, please refer to the Data Retention Policy or contact the Privacy Officer.

## 14. YOUR RIGHTS

14.1 Under the data protection laws, you have legal rights in relation to your personal data:

14.1.1 **To be informed** – We must make this privacy policy (sometimes referred as to the privacy notice) available to you and be transparent over how we process your data.

14.1.2 **Access** – You are entitled to know what details we hold about you and why (please see below clause 14).

14.1.3 **Rectification** – We are obliged to correct or update your details without delay provided you make the request in writing, clearly specifying which data is incorrect or out of date.

14.1.4 **Erasure** – This is also known as the right to be forgotten. You have the right to require us to erase your personal data under specific circumstances. A request for deletion will be decided on a case-by-case basis.

14.1.5 **Restrict processing** – You have the right to 'block' or suppress our processing of your personal data.

14.1.6 **Portability** – You have the right to obtain the personal data that you have provided to us in a commonly used machine-readable format and reuse it with a different organisation.

14.1.7 **Object** – You have the right to object to us processing your data in certain circumstances. However, we may still be allowed (or required) to process your personal data if we can show you that we have a compelling reason for doing so.

14.1.8 **Rights in relation to automated decision making and profiling** – We do not use automatic decision making or profiling.

14.1.9 **Withdraw consent** – Where you have given us consent to process your personal data, you can withdraw that consent at any time. We do not penalise individuals who wish to withdraw consent and we act on withdrawals of consent as soon as we can.

14.2 Should you wish to exercise your data protection rights, please contact the Privacy Officer.

## 15. SUBJECT ACCESS REQUESTS (SAR)

15.1 You are entitled to know about how we hold your personal data and why. We strive to be as open as we can be when granting you access to your data.

15.2 You may raise a formal request with the Privacy Officer. If we do not hold information about you, we will confirm this in writing at the earliest opportunity. If we do hold your personal data, we will respond in writing. Our response will:

15.2.1 confirm that we process your data;

15.2.2 verify the lawfulness and the purpose of the processing;

15.2.3 confirm the categories of personal data we process;

15.2.4 confirm the type of recipients to whom the personal data have been or will be disclosed; and

15.2.5 let you have a copy of the data in a format we deem suitable or as reasonably required by you.

## 16. CHANGES TO THIS PRIVACY POLICY

16.1 We keep our policies under regular review. This version was last updated in October 2026.

# Redruth Town Council
# Member Information Access

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## 1. INTRODUCTION

1.1 Redruth Town Council (**"the Council", "we" or "us"**) recognises that Members require timely, relevant and sufficient information to carry out their constitutional, decision-making, scrutiny and civic functions effectively.

1.2 The purpose of this policy is to set out how Members may request, access, use and handle Council Data in connection with their Council role, while ensuring that information is shared lawfully, proportionately and consistently with the Council's obligations of confidentiality, transparency and information governance.

## 2. DEFINITIONS

2.1 The following definitions in this policy:

| | |
|---|---|
| **Council Data** | information about us, our clients and other Council connections, whether confidential, proprietary or private, held, used or transmitted in any forms including written, spoken and electronically. |
| **Members** | Redruth Town Councillors and those with civic or ceremonial roles such as the Town Mayor and Town Crier of Redruth Town Council. |
| **Content** | any materials, information and communications including but not limited to email (both outgoing and incoming), telephone conversations, voicemail recordings, instant messages and social media postings, created, transmitted, received, printed, stored or recorded during the course of Council business or on our behalf. |
| **Device** | a smartphone, tablet, handheld computer, and any accompanying software or hardware. |
| **Personal Data** | any information relating to an identified or identifiable natural person, be it directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **Systems** | smartphones, mobile or cellular phones, tablets, and laptop or notebook computers. |

## 3. PERSONNEL RESPONSIBLE FOR THIS POLICY

3.1 The Town Clerk and the DPO shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

3.2 Members are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the Town Clerk and DPO.

3.3 Members will receive periodic training on information governance, scrutiny practice and lawful handling of data.

## 4. SCOPE OF THIS POLICY

4.1 Members require timely, relevant and sufficient information to discharge scrutiny and assurance roles effectively.

4.2 This policy aims to work in conjunction with the Code of Conduct and relevant guidance (including but not limited to Local Government Association Guidance) to set out rules regarding information use and access.

4.3 Redruth Town Council must ensure information is easily navigable, accessible and accurate, so that Members are able to perform their constitutional role. For this purpose, it will endeavour to put in place arrangements to regularly (through the Council and Committee meeting structure) share information (such as key performance, financial and governance information) with Members that will help them to understand how the authority is run and reduce the number of active requests for information under this Policy.

4.4 This policy applies to requests for, and use of, Council Data by Members where that information is required for a proper Council purpose. It explains the categories of information that may be made available, the routes for requesting information, and the circumstances in which access may be limited, refused, redacted or subject to safeguards.

4.5 Breach of this policy may lead to a Code of Conduct investigation. In some rare cases, it may also lead in some cases to possible criminal charges.

4.6 Members must only access and use Council Data for proper Council purposes, and not for personal, political campaigning, commercial or other unrelated purposes. Information must not be further disclosed or circulated without authority, and remains subject to applicable data protection, confidentiality and information governance requirements. Members should assume that information provided under this policy may be confidential,

contain personal data or be exempt from publication unless they are expressly advised otherwise.

4.7 Where a suspected breach of this policy is investigated, Members are expected to co-operate with any reasonable enquiries, including enquiries relating to the handling, disclosure, retention or onward sharing of Council Data.

## 5. HOW INFORMATION IS MANAGED

5.1 Redruth Town Council process and manage numerous categories of information. Generally these are:

5.1.1 Publicly Available Information.

5.1.2 Information made available to all Members..

5.1.3 Exempt from Publication.

## 6. PUBLICLY AVAILABLE INFORMATION

6.1 Some information required by Members may also be made public.

6.2 Although the right exists in law, we hope that this Policy means that Members should not need to rely on information access right, such as FOIA or EIR in securing information necessary to their role. However, your rights in this regard shall never be restricted by the Council and any request of this nature shall be handled in accordance with our Subject Rights and Information Access Policy.

6.3 The Council will continue to meet its obligations under the Local Government Transparency Code 2015, which requires publication of prescribed classes of open data relating to organisational performance, expenditure and governance. Information published under the Transparency Code will be made available to all Members through the Council's website. Where additional contextual explanation is required to support effective scrutiny, Redruth Town Council will provide accompanying summaries or reports to ensure that Members can interpret the material accurately and in accordance with the statutory purpose of publication.

## 7. INFORMATION AVAILABLE TO ALL MEMBERS

7.1 Members will be given access to information:

7.1.1 to which they are entitled under law;

7.1.2 prescribed classes of information set out within Local Government Transparency Code 2015 (see 6 above); or

7.1.3 such other constitutional arrangements as may be adopted by the Council from time to time.

Access to personal data is not automatic merely by virtue of being a Member. Where information contains personal data, access will be limited to that which is necessary and proportionate for the Member to discharge their Council function.

7.2 *Entitlements under law*

Members have the following rights to information under law (including but not limited to):

- Right to inspect under Local Government Act(s) 1972;
- Where applicable, Local Authorities (Executive Arrangements) (Meetings and Access to Information) (England) Regulations 2012;
- Accounts and audit regulations;
- As with any other member of the public, Freedom of Information Act 2000 and Environmental Information Regulations 2004; and
- As with any other data subject, Data Protection Act 2018 / UK GDPR

7.3 *Entitlements under "need to know"*

7.3.1 Members may have a legitimate "need to know" where the information requested is reasonably required to enable them to discharge a specific Council function, including decision-making, oversight, scrutiny, audit or assurance. The Town Clerk or Deputy Town Clerk will assess each request by reference to the purpose of the request, the Member's role or committee function, the relevance of the information to that function, and whether disclosure is necessary and proportionate.

7.3.2 Where a request is made for oversight or scrutiny purposes, the request will be considered in light of the principles of effective

scrutiny, including the need to support transparent, accountable and informed decision-making. Access may be refused, limited, redacted or made subject to safeguards where the request is not supported by a proper Council purpose, is disproportionate, or would involve disclosure of exempt, confidential or personal data without an appropriate lawful basis.

7.3.3 Any disclosure of information must be supported by relevant local government legislation and, where personal data is involved, must comply with the UK GDPR and Data Protection Act 2018.

## 8. EXEMPT FROM PUBLICATION

8.1 Certain information is exempt from publication under Schedule 12A of the Local Government Act 1972. This includes:

8.1.1 information relating to a particular individual;

8.1.2 information which is likely to reveal the identity of an individual;

8.1.3 information relating to the financial or business affairs of any particular person (including the authority holding that information) information relating to any consultation or negotiations, or contemplated consultations or negotiations, in connection with any labour relations matter arising between the authority or a minister of the crown and employees of, or office holders under, the authority;

8.1.4 information in respect of which a claim to legal professional privilege could be maintained in legal proceedings;

8.1.5 information which reveals that the authority proposes –

(a) to give under any enactment a notice under or by virtue of which requirements are imposed on a person; or

(b) to make an order or direction under any enactment; or

8.1.6 information relating to any action taken or to be taken in connection with the prevention, investigation or prosecution of crime.

8.2 In applying Schedule 12A to the Local Government Act 1972, the Council will comply with its obligations under Part VA of the Local Government Act 1972, including but not limited to its duties relating to public access to meetings, agendas, reports and background papers.

8.3 Any determination that information is exempt will be made strictly in accordance with the statutory exemptions. This shall be applied narrowly, having regard to the Council's duties of transparency, reasoned decision-making and, where applicable, public-interest considerations.

8.4 Members must not disclose or circulate exempt or confidential information in any circumstances. This includes disclosure during open committee meetings or inclusion within open agendas or minutes. Such matters may only be considered within the confidential section of Council meetings, typically issued under "Yellow Papers" which is the Part II of council and Committee meetings or equivalent restricted documentation. Where exempt information is required, its use should be limited to what is strictly necessary for the purpose of the decision or scrutiny being undertaken. For more information on this, please review the Council's relevant Standing Orders distributed or made available on our website.

8.5 Any unauthorised disclosure, distribution or onward circulation of exempt or confidential information may result in a Code of Conduct complaint.

8.6 The proper and lawful use of personal information is critical to Council operations and the protection of individual rights. Unlawful use and disclosure of personal information may expose both the individual Members and the Council to regulatory enforcement action the Information Commissioner, as well as potential civil claims by affected individuals.

## 9. MAKING REQUESTS FOR INFORMATION

9.1 Requests for information may be made individually or by a chair on behalf of a committee. Such requests may be made, in writing, to:

9.1.1 Admin@redruth-tc.gov.uk where the information requested is suspected to be publicly available;

9.1.2 the named Officer for classes set out within Schedule 1; or

9.1.3 the Town Clerk or Deputy Town Clerk for all other types of information.

9.2 Requests to junior officers will automatically be rejected as those officers are not granted authority to disclose information.

9.3 Access decisions will always be interpreted to support accountable and transparent decision-making, except where a request has no clear purpose, where there is an illegitimate motivation or is disproportionate to Council

resources. The Council will work with the requestor to create exercisable requests.

9.4 Requests for information need to be:

9.4.1 Clear and specific;

9.4.2 Given with plenty of notice (unless there is a justifiable emergency situation);

*Disclosure of information*

9.5 Information must be provided to Councillors in an accurate, timely and complete manner. Redruth Town Council will present this information in an accessible format.

9.6 Redruth Town Council will inform a requestor of expected response time, as soon as reasonably practicable following receipt of a request.

9.7 Documents may contain a mixture of different classes of information, such as exempt and non-exempt information. The Town Clerk or Deputy Town Clerk shall, in their sole discretion, decide on the most suitable method of delivery of information to Members and shall be permitted to deliver information in a format necessary to avoid inadvertent disclosure of exempt or confidential information, such as extraction of relevant information (i.e not providing a document, but an excerpt of the document), summarisation or by providing redacted documents.

9.8 Members must use information responsibly, proportionately and exclusively for proper Council purposes. This does not include campaigning or personal purposes.

*Confidentiality undertakings*

9.9 Where necessary and proportionate to do so, the Town Clerk may seek confidentiality undertakings from any Members to further protect information to be disclosed.

**Schedule 1: Information Classes**

| Types | Examples | General Distribution | Limitations | Request Officer |
|---|---|---|---|---|
| **Organisational Effectiveness Information** | Performance Information (not relating to individuals), Financial Information (not relating to individuals), Risk Information, Third-Party reporting and review documentation and Project/Service Information | Not routinely distributed | Members who are on a specific committee or in the case of a full council issues – all members | Town Clerk and Deputy Town Clerk |
| **Personal Data Information** | Information relating to identifiable individuals, including but not limited to Officers of the Council. | Not routinely distributed | Disclosure must be in accordance with Data Protection Legislation. | Town Clerk and Deputy Town Clerk |
| **Decision-making Information** | Reports, background papers and documents, research and business cases. | Part 1 published Council Papers | Members who are on a specific committee or in the case of a full council issues – all members | Town Clerk or Deputy Town Clerk |

| | | | | |
|---|---|---|---|---|
| | | Part 2 minutes published | Summary of recorded decisions only | |
| **Governance Information** | Agendas. Minutes and reports (many of which will be made available via our Website), Council-related constitutional documents, evidence of governance effectiveness and any other relevant information. | Part 1 published Council Papers | No limitation within boundaries of available Part 1 information. | Town Clerk or Deputy Town Clerk |
| **Prescribed classes of information under Local Government Transparency Code 2015** | Local government transparency code 2015 - GOV.UK | All Members (via Website) | Limited to prescribed datasets. Additional contextual information may be provided upon request, subject to statutory constraints. | Town Clerk and Deputy Town Clerk (responsible for transparency-code publication). |

# Redruth Town Council
# Social Media Policy

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## 1. ABOUT THIS POLICY

1.1 This policy applies to all employees, officers, consultants, contractors, volunteers, interns, casual workers, and agency workers of the Council (the **Council**). It also applies to Councillors (Members) and those with civic or ceremonial roles such as the Town Mayor and Town Crier. These groups are collectively known as "**Council Representatives**" for the purpose of this Policy.

1.2 This policy is in place to minimise the risks to the Council (and Council Representatives) ("the **Council**") through use of Social Media Platforms (as defined below).

1.3 This policy deals with the use of all forms of social media, including but not limited to Meta (Facebook and Instagram), LinkedIn, Whatsapp, X (Twitter), Wikipedia, TikTok and all other social networking sites, internet postings, forums and blogs (collectively known as **Social Media Platforms** under this policy). It applies to use of Social Media Platforms for business purposes as well as personal use that may impact the Council in any way.

1.4 This policy does not form part of any employee's contract of employment, and we may amend it at any time.

## 2. STATEMENT OF PURPOSE

2.1 The availability and use of social networking applications brings opportunities to understand, engage and communicate with our audiences in new ways, the Council must use these technologies and services effectively and flexibly.

2.2 It is also important that the Council balances this with its duties to its service users and the wider community, as well as its legal responsibilities and its reputation.

2.3 The Council will use Social Media Platforms in a safe, appropriate and purposeful way to engage and interact with the public.

2.4 The Council's use of Social Media Platforms will always be consistent with the Council's duty to safeguard children, young people and vulnerable adults, in accordance with relevant statutory requirements and guidance.

2.5 The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

2.6 The purpose of this policy is:

2.6.1 To minimise the reputational, legal and governance risks to the Council and Council Representatives arising from the use of Social Media Platforms in a professional (Council-related) capacity;

2.6.2 To enable the safe use of Social Media Platforms for communication, engagement, customer service and service delivery;

2.6.3 To ensure a consistent approach is applied across the Council focused on achieving key objectives, promoting public transparency and trust and that the reputation of the Council is not adversely affected; and

2.6.4 To ensure that individuals across Social Media Platforms can clearly distinguish where information provided is legitimately representative of the Council.

## 3. WHO IS RESPONSIBLE FOR THIS POLICY?

3.1 The Town Clerk has overall responsibility for the effective operation of this policy. The Senior Management Team has delegated responsibility for overseeing its implementation. Questions about the content of this policy or suggestions for change should be reported to the Town Clerk.

3.2 You should refer any questions you may have about the day-to-day application of this policy (including reporting the misuse of Social Media Platforms) to your line manager**.**

3.3 This policy has been formally adopted by the Full Council and is to be reviewed annually by the Town Clerk in consultation with Full Council.

## 4. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

4.1 You should never use Social Media Platforms in a way that breaches any of our other policies (and, where applicable, Cornwall Council's policies that we are contractually bound to adhere to). For example, you are prohibited from using Social Media Platforms to:

4.1.1 breach of our Safeguarding Policy;

4.1.2 breach any of our IT, security, confidentiality or data-protection policies (including but not limited to our Privacy Notice, the Internal Data Protection Policy, Data Subject Rights and Information Access Policy, Breach and Escalation Policy and the Member Information Access Policy);

4.1.3 breach any obligations we may have with respect to the rules of relevant regulatory bodies;

4.1.4 breach any obligations contained in those policies relating to confidentiality;

4.1.5 breach our disciplinary procedures;

4.1.6 harass or bully other staff in any way;

4.1.7 unlawfully discriminate against other staff or third parties;

4.1.8 breach our Data Protection Policy (for example, you should never disclose personal information about a colleague online); or

4.1.9 breach any other laws or regulatory requirements.

4.2 If you breach any of the above policies, you will be subject to relevant action (such as disciplinary action up to and including termination of employment for employees or commencement of Code of Conduct breach processes in respect of Councillors).

## 5. PERSONAL USE OF SOCIAL MEDIA PLATFORMS

5.1 Use of your own personal Social Media Platforms during working hours is prohibited unless use is work-related or takes place during authorised breaks.

5.2 This policy is designed to cover Council-related use of Social Media Platforms, including:

5.2.1 Council Representatives use of Social Media Platforms as communication tools during the course of their official role connected with the Council.

5.2.2 Access to Social Media Platforms by Council Representatives in the course of their professional duties from devices on the Council's network. Examples include, but are not limited to, monitoring feedback about a service (e.g. TripAdvisor reviews, Facebook comments) or accessing materials to support learning and development (e.g. training videos on YouTube).

5.2.3 Participation on Social Media Platforms not managed by Council Representatives where contributions are posted directly in a professional capacity (e.g. contributing to a professional forum). Contributions include, but are not limited to, text, photographs and video.

5.3 This policy also sets out guidance on personal use of Social Media Platforms, to the extent that such use has a direct impact on the function and reputation of The Council.

## 6. RESTRICTIONS AND PROHIBITED USE

6.1 Council Representatives must not use Social Media Platforms for any of the following prohibited/restricted purposes**:**

### 6.2 Libel

6.3 Libel concerns "lasting" forms of publication such as print, online or broadcasting which adversely affects a person's reputation. Broadcast to the public, and publication on Social Media Platforms, of such material can give rise to actionable claims against the person who writes or publishes the content (including claims for damages and injunctions). If you use Social Media Platforms, websites or systems connected with the Council, the claimant may also argue that the Council is liable. For this reason, libellous statements made Council Representatives are strictly prohibited.

### 6.4 Intellectual Property Rights

Due to their interactive nature, our Social Media Platforms and websites can present a risk of intellectual property infringement. The most common forms of IP encountered are copyright (including written word, images including photography, art) and trademarks (such as logos). Where intellectual property exists, it is likely that permission to use those works, trademark or logo is needed. For this reason, use of third-party protected material is strictly prohibited unless permission of the Town Clerk is sought.

For the avoidance of doubt, data owned by, or derived from, Council systems (including images, video and text) or employees acting during the course of their employment is likely to constitute Council-owned intellectual property and must only be used for Council-approved purposes, unless advance permissions are obtained from the Town Clerk.

### 6.5 Data Protection

*Please see “Guidance on using Personal Data on Social Media Platforms” below.*

### 6.6 Political Content

The Council must remain politically neutral in its activities across Social Media Platforms and websites. The Council cannot promote any candidate in elections, parties, campaigns or political messages.

Councillors may maintain their own accounts on Social Media Platforms, but in doing so they are responsible for their own conduct on those platforms. We offer Councillors guidance on this below.

6.7 **Other restrictions**

6.7.1 Council Representatives must not set up any new account on behalf of the Council on any Social Media Platform without approval of their line manager. All accounts FOR Social Media Platforms must be logged by the Town Clerk or Deputy Town Clerk.

6.7.2 Council Representatives must avoid making any communications via Social Media Platforms that could damage our interests or reputation, even indirectly.

6.7.3 Council Representatives must not use Social Media Platforms to defame or disparage us, other Council Representatives or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

6.7.4 Council Representatives must not express opinions on the Council's behalf via Social Media Platforms, unless expressly authorised to do so by your manager or the Town Clerk. You may be required to undergo training to obtain such authorisation.

6.7.5 Council Representatives must not use any Social Media Platforms or any the Council managed website to upload, share, repost or host any content that is pornographic, violent, or otherwise obscene. To do so would be a criminal offence.

6.7.6 Council Representatives must not use any Social Media Platforms or any website to incite or encourage any criminal behaviour or unlawful activity. This includes (but is not limited to) violence, harassment, discrimination, inciting hatred, encouraging disorder or defamation. This can include indirect or contributory messaging, jokes or comments that could be reasonably interpreted as promoting, condoning or encouraging.

6.7.7 Council Representatives must not post comments about sensitive council-related topics including but not limited to confidential information, information acquired under "yellow papers" or other publicly exempt information and intellectual property. Posts that reveal confidential Council discussions, demonstrate predetermination, or show improper reasoning relating to council

decisions may expose you and the Council to serious legal consequences including, in the Council's case, judicial review.

6.7.8 Council Representatives must not include our logos or other trademarks in any Social Media Platform posting or in your personal profile (or campaigning page).

6.7.9 Council Representatives should never provide references for other individuals on social or professional networking sites. These references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

6.8 Any misuse of Social Media Platforms should be reported to the Town Clerk.

## 7. GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA PLATFORMS

7.1 Council Representatives should make it clear in any personal profile posting that could reasonably be interpreted as 'connected' to your role with the Council, that you are speaking on your own behalf. Write in the first person and use a personal profile set up under a personal email address.

7.2 Council Representatives must be respectful to others when making any statement on Social Media Platforms and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

7.3 Should Council Representatives disclose your affiliation with the Council on your profile or in any Social Media Platform postings, you must state that your views do not represent those of the Council (unless you are authorised to speak on our behalf as set out in paragraph 6.7.4). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

7.4 If Council Representatives are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

7.5 If Council Representatives see any online or public content that disparages or reflects poorly on the Council, you should contact the Town Clerk without delay.

7.6 For the avoidance of doubt, the Council has identified the following permitted uses of Social Media Platforms and websites:

7.6.1 Distribute public agenda, minutes and dates of meetings;

7.6.2 Advertise Council activities and activities undertaken by the Council on behalf of other, such as the Library (subject to contract with Cornwall Council).

7.6.3 Upload approved press releases and messages.

7.6.4 Advertise of vacancies.

7.6.5 ‘Share’, ‘repost’ or ‘retweet’ information from partner bodies, organisations or community groups subject to the content not breaching any requirement of this Policy; and

7.6.6 Take public questions, queries or comments. Where possible, such queries should be taken out of the public space, and into a private, secure method of communication as quickly as possible.

## 8. GUIDANCE ON USING PERSONAL DATA ON SOCIAL MEDIA PLATFORMS AND THE COUNCIL WEBSITES

8.1 Using any form of personal data across our Social Media Platforms and websites will trigger the need to ensure that such use meets the requirements of data (use and access) 2025, UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (together “**Data Protection Laws”**).

8.2 Personal data commonly used on Social Media Platforms includes (but is not limited to) individual’s names, job roles and images. This includes the personal data of Council Representatives and participants in Council activities and initiatives.

8.3 We must ensure that any use of personal data across our digital assets always remains compliant with Data Protection Laws, this includes meeting the data protection principles of:

8.3.1 Lawfulness, fairness and transparency,

8.3.2 Purpose limitation

8.3.3 Data minimisation

8.3.4 Accuracy

8.3.5 Storage limitation

8.3.6 Integrity and confidentiality (security)

8.3.7 Accountability.

8.4 Our Data Protection Policy, together with our Privacy Notice, explains how the Council meets its legal obligations in this regard.

8.5 Our permitted uses of personal data for Social Media Platforms and website purposes are set out in our Record of Processing Activities. Any activity not recorded within this ROPA is not permitted by the Council, and you must seek Town Clerk approval before undertaking the activity.

8.6 **Photography**

8.6.1 A common issue when using Social Media Platforms is the handling of images taken at Council meetings or events. The Council and Council Representatives must balance the benefits of using photography to support their activities, and respecting privacy of individuals, including fellow Council Representatives.

8.6.2 Both the Council and its Representatives must adhere to strict privacy and safeguarding standards when publishing images online. The Council has formal procedures in place that set out when and how images can be lawfully taken and used. These procedures do not normally allow Council Representatives to take their own photographs of individuals or to use images on personal or non-Council related Social Media Platform accounts or websites.

8.6.3 Taking or using images independently, outside the Council's authorised processes, may create safeguarding risks for the individual involve or lead to complains of data misuse against you and/or the Council.

8.6.4 To aide Council Representatives' use of images, the Council shall support Council Representatives by:

(a) Informing Council Representatives in advance if non-official photography is permitted.

(b) Circulating images which can be publicly circulated (including guidance on circulation and any applicable restrictions).

(c) Provide clear instructions on how promotional materials, including images, may be used. Council Representatives must not deviate from those instructions.

(d) Maintaining a central, secure image library for approved use.

(e) Ensuring all images taken by the Council meet the requirements of the Data Protection Policy.

(f) Offering practical support to those seeking to use images and online content.

8.6.5 By taking or using independent images without regard to this Policy, you understand that you do so:

(a) without the authority of the Council;

(b) in the knowledge that you may be identified as a Data Controller under Data Protection Laws, resulting in (i) your need to meet the relevant data protection principles, including transparency to individuals, (ii) allocation of a 'lawful basis' and, (iii) and with an obligation to respond personally to data subject right requests, complaints, or regulatory enquiries;

(c) at your own risk, including potential exposure to complaints, safeguarding concerns or legal claims by individuals;

(d) in breach of this Policy and the Council's Data Protection Policy, which may result in disciplinary action (for employees) or Code of Conduct investigations (for applicable Council Representatives).

## 9. GUIDANCE FOR COUNCILLORS, TOWN MAYOR AND TOWN CRIER ON NON-COUNCIL RELATED SOCIAL MEDIA PLATFORM USE

9.1 If you are already using, or planning to use, Social Media Platforms in connection with your position as a Councillor, Town Mayor or Town Crier, you should ensure that you are familiar with this guidance and your duties under the Code of Conduct and Data Protection Law.

9.2 The Council welcomes your use of Social Media Platforms:

9.2.1 in a personal capacity;

9.2.2 to communicate to constituents and the wider community;

9.2.3 to support your community leadership position;

9.2.4 to partake in positive, polite and constructive debate and public discussion on community issues; and

9.2.5 to support your political activities and campaigning.

9.3 It is important to understand the legal distinction between your use of Social Media Platforms as a Council Representative and use for political or personal purposes. You will be personally responsible for the content they publish on any Social Media Platform and you are still subject to the Code of Conduct on Social Media Platforms where there is an explicit link between the content posted and council business or your role.

9.4 To ensure a clear, distinct and safe public communications and engagement, you should consider the following:

9.4.1 keep separate Social Media Platform accounts to distinguish between your official role and your personal life to avoid ‘blurred identities’. The Local Government Association recommend setting up your personal account as a “person or user” and your official role as a “page or business”. We also recommend a separate political or campaigning page, if required, to ensure your ‘official role’ accounts do not become confused with political messaging and campaigning issues, while preserving the privacy of your personal accounts;

9.4.2 ensure robustness of safety by using different passwords where possible, not using your Council email (which is on public record) to set up the account; and use two-factor authentication where possible;

9.4.3 follow Civility in Public Life and LGA Digital Citizenship principles;

9.4.4 not engage in rumours, personal ‘attacks’ or smear / misinformation campaigns, either as a perpetrator or victim. We encourage you to document and, where possible, screenshot any malicious material as this may be useful for future disciplinary or legal action. If you are directly impacted by such a campaign and wish to respond, the Town Clerk can assist you with any public actions;

9.4.5 be mindful that ‘what goes online, stays online’ – you immediately loose control of any information uploaded, nor can you alter how something is construed once circulate/posted. Where you attempt to delete problematic material, no deletion process is 100% effective. This creates risks for you individual, and the Council. You must be confident in the lawfulness and suitability of what you put into the public space;

9.4.6 be aware that public life brings with it security and safety considerations. Do not upload information that may disclose information that should be protected, such as your information and images relating to your friends/relationship network, your personal address, personal contact details. This also applies to information that may potentially harm others and to do so may place you personally in breach civil laws or at risk of criminal prosecution;

9.4.7 be aware of the risk of misinformation and the misleading impact of AI generated 'fake' content. You should take reasonable steps to verify your sources before circulating information publicly; and

9.4.8 take caution with granting accesses to your Social Media Platform accounts. Loss of control of Social Media Platform accounts can lead to significant reputational damage and loss of public trust. It is also incredibly difficult to recover 'stolen' accounts.

9.5 Council Representatives should not divulge information that is confidential or subject to public disclosure exemptions using any Social Media Platform or website.

9.6 Council Representatives should make every effort to uphold public trust when communicating via any Social Media Platform. We outline steps that the Council would ask that you consider.

| **Account type/activity** | **Personal Account** | **Campaigning Page** | **Official Role Page** |
|---|---|---|---|
| **Disclaimer recommended** | "This is my personal account and views expressed are my own and do not represent The Council. For official council business, please visit [Official Page]" | "This is my political campaigning page. Views expressed are my own and relate to my political activities only. This page is not affiliate with, or endorsed by, The Council"<br><br>For privacy reasons, do not recommend you | ""Councillor for Ward]. Member of [NAME] Committee for The Council. This is my official page for council-related updates. For campaigning/political please visit [Political Page]".<br><br>For privacy reasons, do not recommend you referencing your personal accounts. |

| | | | |
|---|---|---|---|
| | | referencing your personal accounts. | |
| **Responsibility for content** | You | You | You, and when related to Council business, the Council |
| **Use of personal data, Data Protection Legislation considerations and data roles.** | N/A – subject to exemption in most cases. | You will likely act as Data Controller for this purpose. Please review Guidance for the use of personal data in political campaigning \| ICO. | You, and when related to Council business, potentially the Council. Please review the following guidance to better understand your legal duties as a data controller: Guidance for the use of personal data by elected representatives in carrying out constituency casework \| ICO. |
| **Types of content** | Personal life, hobbies, interests. Not representing your role or the Council in any capacity. | Political messaging, (where applicable) party political views, election aligning, promotion of political activities and manifesto issues. | Official Council information (subject to the requirements of this policy), community issues, service updates, engagement with constituents on Council business.<br><br>A high standard of accuracy, neutrality, integrity, non-political tone are expected. |
| **Limitations** | • You cannot use Council | • No use of Council | • You may use Council |

| | | | |
|---|---|---|---|
| | resources (equipment, email address, logos, images, systems)<br><br>• You must not imply that you are speaking on behalf of the Council or have Council support or endorsement.<br><br>• You must not be used to disclose confidential council information, Council employee information or data (including personal data) under controllership of the council.<br><br>• You must follow general moral standards of respectful conduct. | images or information without Town Clerk written consent.<br><br>• You cannot use Council resources (equipment, email address, logos, images, systems)<br><br>• You must not imply that you are speaking on behalf of the Council or have Council support or endorsement.<br><br>• Where applicable, must comply with election period rules, Data Protection Laws and Code of Conduct.<br><br>• Must not make misleading claims. | information and data, as permitted by the Code of Conduct and this Policy.<br><br>• You must comply with Council Policies, Data Protection Laws and the Code of Conduct.<br><br>• Must not place the Council in breach of its obligation under Code of Recommended Practice on Local Authority Publicity in 2011.<br><br>• Content is potentially subject to Council FOIA and EIR information access requirements.<br><br>• Must be used for the benefit of all constituents. |

## 10. TRAINING

10.1 Training on Social Media Platform usage and other related topics such as Civility in Public Life will be made available to staff on request and in consultation with line managers on induction and as part of the appraisal system.

10.2 This Policy, together with applicable guidance such as the LGA Checklist for Councillors, will also be made available to each Council Representative at the beginning of their relationship with the Council. Any updates will also be circulated following approval.

## 11. BREACH OF THIS POLICY

11.1 Breach of this policy may result in disciplinary action up to and including dismissal (in the case of employees) or Code of Conduct investigations (for applicable Council Representatives). Any member of staff suspected of committing a breach of this policy will be required to reasonably co-operate with our investigation.

11.2 You may be required to remove any Social Media Platform content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action or a Code of Conduct investigation. Reach of this policy may result in disciplinary action up to and including dismissal (in the case of employees) or Code of Conduct investigations (for applicable Council Representatives). Any member of staff suspected of committing a breach of this policy will be required to reasonably co-operate with our investigation.

11.3 You may be required to remove any Social Media Platform content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action or a Code of Conduct investigation.

# Redruth Town Council
# Data Processing Agreement (Template)

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## DATA PROCESSING AGREEMENT - SUMMARY

This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing services under the Service Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

### Parties

The below parties have agreed to enter into the Data Processing Agreement and together are referred to as the parties:

**Customer:**

| | |
|---|---|
| **Name** | Redruth Town Council |
| **Address** | Civic Centre, Alma Pl, Redruth TR15 2AT |
| **SPoC name** | [INSERT] |
| **SPoC email** | [INSERT] |
| **SPoC phone** | [INSERT] |

**Provider:**

| | |
|---|---|
| **Name** | [INSERT] |
| **Company Registration** | [INSERT] |
| **Address** | [INSERT] |
| **SPoC name** | [INSERT] |
| **SPoC email** | [INSERT] |
| **SPoC phone** | [INSERT] |

### Service Agreement

### Particulars

- **Subject matter of processing:** [Short description, for example name of the service or description of the Services Agreement]
- **Duration of Processing:** [Periods for which the services are being provided]
- **Nature of Processing:** [Description of the type of processing such as data collection, storage, sharing and so on]
- **Business Purposes:** [Description of the processing purpose(s) – for example processing for HR purposes, recruitment, direct marketing and so on]
- **Personal Data Categories:** [Set out types of personal data such as names, contact details, pay details, images and so on]

- **Data Subject Types:** [Set out categories of data subjects such as employees, customers, students and so on]

**Security Measures**

- **Physical access controls:** [Set out measures to restrict physical access to buildings, rooms, or devices]
- **System access controls:** [Set out policies and technologies to manage who can access computer systems]
- **Data access control:** [Set out rules and tools to control who can view or use the shared personal data]
- **Transmission controls:** [Set out methods to secure data during transfer between systems]
- **Input controls:** [Set out procedures to ensure personal  data entered into systems is accurate and authorised]
- **Data backups:** [Set out processes to create copies of data for recovery in case of loss]
- **Data segregation:** [Set out practices to keep different types of data separate for security and compliance]

**Register of Sub-Processors**

[INSERT]

By signing below the parties agree to share data on the terms set out in this Agreement.

| **Start date:** | |
|---|---|
| **Signed by Customer** | **Signed by Provider** |
| Authorised Signature: | Authorised Signature: |
| Date: | Date: |
| Printed Name: | Printed Name: |
| Position: | Position: |

## AGREED TERMS

### 1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

**Agreed Purposes**: the services to be provided by the Provider to the Customer as described in the Service Agreement and any other purpose specifically identified in **Error! Bookmark not defined.**the Summary.

**Commissioner**: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

**Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing**: have the meanings given in the Data Protection Legislation.

**Controller:** has the meaning given in section 6, DPA 2018.

**Data Protection Legislation**: all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; [[and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications);] [and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party].

**Data Subject**: the identified or identifiable living individual to whom the Personal Data relates.

**Personal Data**: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

**Processing, processes, processed, process**: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

**Personal Data Breach**: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

**Processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

**Single Point of Contact or "SPoC"**: the persons or categories of persons that the Customer authorises to give the Provider written personal data processing instructions as identified in **Error! Bookmark not defined.**the Summary and from whom the Provider agrees solely to accept such instructions.

**Records**: has the meaning given in Clause 12.

**Term**: this Agreement's term as defined in Clause 10.

**UK GDPR:** has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This Agreement is subject to the terms of the Services Agreement and is incorporated into the Services Agreement. Interpretations and defined terms set forth in the Services Agreement apply to the interpretation of this Agreement.

1.3 The Summary forms part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Summary.

1.4 A reference to writing or written excludes fax [and email **OR** but not email].

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

(c) any of the provisions of this Agreement and the provisions of the Services Agreement, the provisions of this Agreement will prevail.

## 2. Personal data types and processing purposes

2.1 The Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Provider is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Provider.

(c) **Error! Bookmark not defined.**The Summary describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.

## 3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions [from Authorised Persons]. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Provider must comply promptly with any Customer written instructions requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires the Provider to process or disclose the Personal Data to a third-party, the Provider must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

3.4 The Provider will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, and information access under Freedom of Information Act 2000 and Environmental Information Regulations 2004 (SI 2004/3391), taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, information access rights, data protection impact assessments and reporting to and consulting with the Commissioner.

3.5 The Provider must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Provider's performance of the Services Agreement or this Agreement.

## 4. Provider's employees

4.1 The Provider will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2 The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness of all of the Provider's employees with access to the Personal Data.

## 5. Security

5.1 The Provider must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Annex B. [The Provider must document those measures in writing and periodically review them at least [INSERT FREQUENCY] to ensure they remain current and complete.]

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

## 6. Personal data breach

6.1 The Provider will immediately and in any event without undue delay notify the Customer in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Provider will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Provider becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Provider will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Provider will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic law.

6.5 The Provider agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

6.7 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Provider caused such, including all costs of notice and any remedy as set out in Clause 6.5.

## 7. Transfers of personal data

7.1 The Provider (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK without obtaining the Customer's prior written consent.

## 8. Subcontractors

8.1 The Provider may not authorise any third party or subcontractor to process the Personal Data.

8.2 The Provider may only authorise a third-party (subcontractor) to process the Personal Data if:

(a) the Customer provides written consent prior to the appointment of each subcontractor;

(b) the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts;

(c) the Provider maintains control over all of the Personal Data it entrusts to the subcontractor; and

(d) the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

8.3 Those subcontractors approved as at the commencement of this Agreement are as set out in **Error! Bookmark not defined.Error! Reference source not found.** Summary. The Provider must list all approved subcontractors in **Error! Reference source not found.** Summary and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.4 Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider which contains terms substantially the same as those set out in this Agreement, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.5 The Parties agree that the Provider will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

8.6 On the Customer's written request, the Provider will audit a subcontractor's compliance with its obligations regarding the Personal Data and provide the Customer with the audit results. Where the Customer concludes reasonably that the subcontractor is in material default of its obligations regarding the Personal Data, the Customer may in writing instruct the Provider to instruct the subcontractor to remedy such deficiencies within [NUMBER] days.

## 9. Complaints, data subject requests and third-party rights

9.1 The Provider must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner [or other relevant regulator] under the Data Protection Legislation.

9.2 The Provider must notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Provider must notify the Customer within **[NUMBER]** days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Provider will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic law.

## 10. Term and termination

10.1 This Agreement will remain in full force and effect so long as:

(a) the Service Agreement remains in effect; or

(b) the Provider retains any of the Personal Data related to the Service Agreement in its possession or control (**Term**).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Service Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 The Provider's failure to comply with the terms of this Agreement is a material breach of the Service Agreement. In such event, the Customer may terminate the Service Agreement effective immediately on written notice to the Provider without further liability or obligation of the Customer.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Services Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation [within [NUMBER] days], either party may terminate the Services Agreement [on not less than [NUMBER] working days OR with immediate effect] on written notice to the other party.

## 11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Services Agreement for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents, materials or Personal Data that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Provider will certify in writing to the Customer that it has deleted or destroyed the Personal Data within [NUMBER] days after it completes the deletion or destruction.

## 12. Records

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 (**Records**).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this Agreement and the Data Protection Legislation and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Provider must review the information listed in the Summary to this Agreement at least once a year to confirm its current accuracy and update it when required to reflect current practices.

## 13. Audit

13.1 The Provider will permit the Customer and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least [NUMBER] days' notice, during the Term. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Customer. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to process the Personal Data.

13.2 The notice requirements in Clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach has occurred or is occurring, or the Provider is in material breach of any of its obligations under this Agreement or any of the Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Agreement or any of the Data Protection Legislation, the Provider will:

(a) [promptly **OR** within [NUMBER] days of the triggering event], conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within [NUMBER] days.

## 14. Warranties

14.1 The Provider warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Services Agreement 's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 5.1.

14.2 The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

## 15. Indemnification

15.1 The Provider agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider or its employees, subcontractors or agents to comply with any of its obligations under this Agreement and/or the Data Protection Legislation.

15.2 Any limitation of liability set forth in the Services Agreement will not apply to this Agreement's indemnity or reimbursement obligations.

## 16. Notice

16.1 Any notice given to a party under or in connection with this Agreement shall be in writing and shall be:

(a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case)

(b) sent by email to the SPoC addresses given in the Summary or an address substituted in writing by the party to be served.

16.2 Any notice shall be deemed to have been received:

(a) if delivered by hand, at the time the notice is left at the proper address;

(b) if sent by pre-paid first-class post or other next working day delivery service, at 9:00am on the second Business Day after posting; or

(c) if sent by email, at the time of transmission, or, if this time falls outside Business Hours in the place of receipt, when Business Hours resume.

16.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This Agreement has been entered into on the date stated in the Summary.

# Redruth Town Council
# Data Protection Impact Assessment (Template)

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | Final |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## WHAT IS A DATA PROTECTION IMPACT ASSESSMENT?

A Data Protection Impact Assessment allows an organisation to identify and minimise the risks posed to Data Subjects, as defined in the UK General Data Protection Regulation, when carrying out a new project. The requirements of the DPIA are set out under Article 35 UK GDPR.

This DPIA is not appropriate for Law Enforcement Agencies or activities **conducted by** local authorities which would mean they are classified as a Law Enforcement Agency.

## HOW TO COMPLETE A DATA PROTECTION IMPACT ASSESSMENT (DPIA)

**Step 1: Complete Identifying Details and Preliminary Systematic Description of Activity.** This section seeks to deliver the information required by both the UK GDPR and the Data Protection Act 2018. Please note that the Assessment Summary should be reserved for the end of the process as this seeks to summarise the outcome.

**Step 2: Complete the Screening**
This process seeks to highlight where a DPIA must be performed, where a DPIA is recommended and where a DPIA may be low risk or exempted.

**Step 3: Complete the Further Systematic Description of Activity.** This further information works in conjunction with the Preliminary Systematic Description to meet the requirements of Article 35 (7) (a) UK GDPR to properly assess the impact of the activity.

**Step 4: Complete the Necessity and Proportionality Assessment**. This information meets the requirements of Article 35(7)(b) UK GDPR.

**Step 5: Complete the Risk to Rights and Freedoms Assessment.** This table enables the asses to meet the requirements of Article 35 (7) (c) UK GDPR and Section 64 Data Protection Act 2018 by identifying the origin, nature, particularity and severity of the risks presented by the activity. For each risk potential impacts and threats are identified, together with the likelihood and severity of those risks and threats, and any measures envisaged to treat those risks are determined (as required by Article 35(7)(d) UK GDPR).

**Step 5: Highlight any additional appraisal techniques required to assess the activity.** Additional appraisal techniques may be required to properly assess this activity to the

standard expected by the DPIA. Please include appraisal considerations and outcomes relevant to this DPIA under this section.

**Step 6: Outcome.** This section aims to record the outcome of the assessment, together with decision details, decision maker details, quality control data and any review requirements. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

## STEP 1(a): IDENTIFYING DETAILS

| | |
|---|---|
| Name of the initiative and number, if applicable | |
| Name, contact information and other identifying details of: | |
| Data controller(s) | |
| Data processor(s), if applicable | |
| Anticipated Data sub-processor(s), if applicable | |
| Scheme Representative | |
| Assessor(s) | |
| Data protection officer(s) (DPO), if appointed | |
| Senior Responsible Officer (SRO), if appointed | |
| Chief information security officer, if appointed | |
| Applicable Supervisory Authority | |
| Level of confidentiality of the Assessment | |
| Date and place of compilation of the report | |
| *[Any other details, as practicable]* | |

## ASSESSMENT SUMMARY

| |
|---|
| [Summary to be added upon conclusion of the assessment] |

## STEP 1(b): PRELIMINARY SYSTEMATIC DESCRIPTION OF ACTIVITY

| | | *Explanation* |
|---|---|---|
| ***Functional Description*** *of the Activity* | | |
| Will the activity involve personal data *(as defined by Data Protection Legislation)* | | |
| **Nature** *(what types of processing operations?)* | | |
| **Scope** | Scale | |
| | Time | |
| **Context** of activity | | |
| **Purpose** of activity | | |
| Categories of **Data Subject** | | |
| Categories of **Personal Data** processed | | |
| **Means** of processing (infrastructure) and assets on which personal data rely *(and by what means? e.g., analogue, digital)* | | |
| Envisioned data flows | | |
| Jurisdiction | | |
| Anticipated Roles | | |
| *[Other information, specify]* | | |

**STEP 2: SCREENING**

These questions are intended to help decide whether a DPIA is necessary and will also highlight where a DPIA is mandated by law. Please refer to the key below to assess your responses.

| | |
|---|---|
| 1. Does the project involve automated decision-making or profiling that produces legal or similarly significant effects on individuals? | |
| 2. Does the project involve large-scale processing of special category data (e.g., health, biometric, racial/ethnic origin) or data relating to criminal convictions or offences? | |
| 3. Does the project involve systematic monitoring of publicly accessible areas (e.g., CCTV, tracking technologies)? | |
| *4.* Will the project involve the collection of new information about individuals? | |
| 5. Will the project compel individuals to provide information about themselves? | |
| 6. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | |
| 7. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | |
| 8. Does the project involve you using new technology which might be perceived as being intrusive to privacy? *(For example, the use of biometrics or facial recognition)*. | |
| 9. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? | |
| 10. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? *(For example, health records, criminal records or other information that people would consider to be particularly private).* | |
| 11. Will the project require you to contact individuals in ways which they may find intrusive? | |
| 12. Does the proposal involve systems or processes that monitor staff or the public? | |

| | |
|---|---|
| 13. Is the processing activity routine and unlikely to result in a high risk to individuals? | |
| 14. Is the processing identical or very similar to one already covered by an existing DPIA? | |
| 15. Is the processing fully covered under an approved code of conduct or certification mechanism that includes DPIA guidance (meaning this DPIA isn't required)? | |
| 16. Is the processing listed by the ICO as not requiring a DPIA? | |
| 17. Is the Data Controller otherwise exempted from the DPIA process? | |

| | | |
|---|---|---|
| Red Box | Yes = DPIA Mandatory | The processing meets one or more criteria under Article 35(3) of the UK GDPR. You must conduct a DPIA. |
| Yellow Box | Yes = DPIA likely required and recommended | The processing may present moderate risks or involve new technologies or practices. A DPIA is likely required by law and strongly advised to ensure compliance and accountability. |
| Green Box | Yes = DPIA Potentially Not Required | The processing is low risk, routine, or already covered by an existing DPIA. You may be exempt, but document your rationale. |

**DPIA SCREENING OUTCOME**

Based on the response to the questions and using the key above, please describe the outcome of this screening exercise.
Where remedial action is required in order to offset the need to carry out a DPIA, this decision, as well as the action to be carried out, must be recorded in a separate document and maintained in your data protection register.

| | |
|---|---|
| **GOVERNING LAW AND APPLICABLE CODES OF CONDUCT** | |

## STEP 3: FURTHER SYSTEMATIC DESCRIPTION OF ACTIVITY

| **ACTIVITY DETAILS** | *Detail* |
|---|---|
| What **categories / types of personal data** will be processed as a result of this activity? | |
| What is the **source** of the data / how is it collected? | |
| How will the data be **stored**? | |
| What is the anticipated **retention period** for storage (if applicable) | |
| Will this data be **shared** with any other party? | |
| What **technological and organisational measures** are in place? | |

## STEP 4: NECESSITY AND PROPORTIONAILITY ASSESSMENT

| | | |
|---|---|---|
| What is the Article 6/9/10 **lawful basis** and Conditions for conducting the proposed activity? | | |
| **Benefits** of activity | for individuals, including data subjects | |
| | for the data controller | |
| | for the society as a whole | |
| **Drawbacks of activity** | for individuals, including data subjects | |
| | for the data controller | |
| | for the society as a whole | |
| **Measures** | | |
| | Have similar or less intrusive activities been considered or attempted? | |
| | How does the proposed activity achieve the Purpose outlined under Stage 1 above? | |
| | How will personal data be limited to the activity only (avoiding function creep?) | |

| | | |
|---|---|---|
| | How will you support data subject rights? | |
| | How will you inform stakeholders that you are conducting this activity? Is it appropriate to consult with Data Subjects and their representatives? | |
| | What measures are taken to ensure that processors comply? | |
| | How are international transfers safeguarded (if applicable) | |

**STEP 5: RISK TO RIGHTS AND FREEDOMS ASSESSMENT**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ***Likelihood of occurrence*** | ***Severity of consequence(s) if risk materialises*** | ***Risk level (score)*** | *Risk response* | *Response plan* | | |
| | | | | | | ***Effect on risk*** | ***Residual Risk*** | ***Measured Approved by Responsible Person*** |
| *ID* | *Risk* | Remote, possible or probable | Minimal, significant or severe | Low, medium or high | *Mitigating Actions* | *(Eliminated/ Reduced/ accepted)* | *(Low/ Medium/ High)* | *Yes/No* |
| **The risks noted under this section are limited to processes arising from the Scheme rather than the use of CCTV more generally.** | | | | | | | | |
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | | | | | | | | |
| | | | | | | | | |

| | |
|---|---|
| DPO / SPO Advice (if required) | [Please input DPO / SPO Advice] |

| | |
|---|---|
| Consultation with the Information Commissioner is mandatory under Article 36 UK GDPR where the DPIA indicates that the processing would result in a high risk to the rights and freedoms of individuals where risks cannot be sufficiently mitigated.<br><br>Detail such consultation here. | |

**Appraisal techniques**, other than the necessity and proportionality assessment, and risk assessment, to be used in the assessment process, if any:

| | | |
|---|---|---|
| Law Enforcement DPIA (LE DPIA) | | |
| Environmental impact assessment (EIA) | ☐ | |
| Privacy impact assessment (PIA) | | |
| Ethics impact assessment | | |
| Social impact assessment | | |
| Health impact assessment | | |
| | | |

**STEP 6: OUTCOME**

| OUTCOME | |
|---|---|
| PENDING | |
| FAIL | |
| PASS | |
| **DECISION DETAIL** | |
| *Please insert reasons and/or requirements* | |
| **OUTCOME REVIEW REQUIREMENTS** | |
| How often will you conduct a **review** of this activity to ensure it is still required? | [Annually] |

| ***Completed by:*** | | ***Authorised By:*** |
|---|---|---|
| Name: | | |
| Role: | | |
| Date: | | |
| Signed: | | |

# Redruth Town Council
# Information Sharing Agreement

Updated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## DATA SHARING FRAMEWORK (PROJECTS) - SUMMARY

This Data Sharing Framework (**Framework**) sets out the principles, obligations and governance arrangements that apply to the sharing of personal data between the Participants for the purposes of the Project. It provides a structured basis for ensuring that any information shared is handled lawfully, securely and consistently, and that each party understands its respective responsibilities when acting as a controller, joint controller or processor under the Project.

### Parties

The below parties have agreed to enter into the Data Sharing Framework and together are referred to as the parties:

**Participant 1:**

| | |
|---|---|
| **Name** | Redruth Town Council |
| **Address** | Civic Centre, Alma Pl, Redruth TR15 2AT |
| **SPoC name** | [INSERT] |
| **SPoC email** | [INSERT] |
| **SPoC phone** | [INSERT] |

**Participant 2:**

| | |
|---|---|
| **Name** | [INSERT] |
| **Company Registration** | [INSERT] |
| **Address** | [INSERT] |
| **SPoC name** | [INSERT] |
| **SPoC email** | [INSERT] |
| **SPoC phone** | [INSERT] |

### Project Details

| | |
|---|---|
| **Project Name** | [INSERT] (“**The Project**”) |
| **Project Commencement Date** | [INSERT] |
| **Link to Heads of Terms** | [INSERT] |

By signing below the parties agree to share data on the terms set out in this Framework.

| **Start date:** | |
|---|---|
| **Signed by Participant 1** | **Signed by Participant 2** |
| Authorised Signature: | Authorised Signature: |
| Date: | Date: |
| Printed Name: | Printed Name: |
| Position: | Position: |

**Summary – Part B**

| **Roles of Parties**<br>The Participants shall have the following data roles throughout the Project. | | | | |
|---|---|---|---|---|
| **Project Activities and subject matter of processing** | **Arrangement Type** | **Data Roles** | **Personal Data Groups** | **Processing Particulars (where applicable)** |
| [TO ADD] | [TO ADD] | [TO ADD] | [TO ADD] | [TO ADD] |
| **Personal Data Groups**<br>[TO ADD] | | | | |
| **Access Restrictions**<br>[TO ADD] | | | | |
| **Lawful bases (and conditions or exceptions for processing of any Special Categories of Personal Data and Criminal Offence) and legal power for data sharing**<br>[TO ADD] | | | | |
| **Agreed Joint Controller Arrangements**<br>[TO ADD] | | | | |

**Contents**


1. Participants ..... **Error! Bookmark not defined.**
2. Introduction ..... 2
3. Framework governance ..... 2
4. Objective ..... 2
5. Purpose ..... 3
6. Duration of Processing ..... 4
7. Framework Principles ..... 4
8. Key personnel ..... 5
9. Compliance with Data Protection Legislation ..... 5
10. Data control ..... 5
11. Controller to Controller Arrangement Obligations ..... 5
12. Controller to Processor Arrangement Obligations ..... 5
13. International Transfers ..... 5
14. Security and training ..... 6
15. Effect of non-compliance with Data Protection Legislation. ..... 7
16. Insurance ..... 7
17. Allocation of cost ..... 7
18. Dispute resolution under the framework ..... 7
19. Third party rights ..... 7
20. Variation ..... 7
21. Waiver ..... 7
22. Severance ..... 8
23. Changes to the applicable law ..... 8
24. Rights and remedies ..... 8
25. Governing law ..... 8
26. Jurisdiction ..... 8
27. Interpretation ..... 8

1. **Parties**

1.1. The parties participating the Project (**Participants**) shall be those listed in Part A of the summary above, unless otherwise agreed between the parties from time to time.

2. **Introduction**

2.1. This Framework has been developed to ensure that information is disclosed and collected appropriately, lawfully and to the highest of standards between Participants and, where permitted, third-parties.

2.2. This Framework aims to establish a consistent approach to data use, sharing and disclosure by governing principles and practices for sharing personal data for the purpose of the Project.

2.3. This Framework will be supplemented by:

2.3.1. the Participants' statutory duties, including but not limited to duties in respect of personal data; and

2.3.2. the Project Terms of Reference.

2.4. Each of the Participants are committed to implementing this Framework in an exemplary and transparent manner and with the highest regard to their legal obligations, the rights of each Data Subject and the overall security of the information it holds.

3. **Framework governance**

3.1. The Participants shall hold the responsibility for oversight and governance of the Framework.

3.2. The SPoCs shall meet at least annually to review the effectiveness of this Framework in relation to the Project, such review shall include:

3.2.1. assessing the efficiency and effectiveness of the Framework; and

3.2.2. ensuring compliance with the Framework and statutory obligations.

3.3. Should any activity listed under Part B of the Summary (**Project Activity**) require variation or removal, each party shall work together in good faith to make any changes that are necessary to this Framework.

4. **Objective**

4.1. In addition to any project objectives set out within the Project Terms of Reference, the Participants shall co-operate to achieve the following data protection and privacy objectives:

4.1.1. To ensure each Participant complies with Data Protection Legislation at all times throughout the Project;

4.1.2. To create an effective, consistent, secure and reliable Framework for data sharing between Participants when required by the Project;

4.1.3. To formalise the contractual basis for information sharing activities and ensure any inherent risks are appropriately managed;

4.1.4. To set out each Participant's respective data roles under Data Protection Legislation (as Controllers, Joint Controllers and/or Processors) in relation to the Project;

4.1.5. To protect Participants from allegations of unlawful use of data, and resulting liability and reputational damage, arising from the Project;

4.1.6. To regulate the secure storage and lawful transfer of Personal Data under the Project, including any resulting international transfers; and

4.1.7. To ensure any disclosures made to third parties are lawfully and efficiently managed.

5. **Purpose**

5.1. This Framework defines the principles and procedures that the Participants shall adhere to and the responsibilities the Participants owe to each other.

5.2. This Framework sets out the arrangements for Personal Data under the Project when an Originating Controller:

5.2.1. discloses Personal Data to another Participant (the **Controller Receiver/s**), who will also act as a Controller in respect of the Personal Data, during a Project Activity (**Controller to Controller Arrangement**); or

5.2.2. instructs another Participant to act as Data Processor in respect of Personal Data in relation to a Project Activity (**Controller to Processor Arrangement**).

5.3. Controller to Controller Arrangements under clause 5.2.1 and Controller to Processor Arrangements under clause 5.2.2 shall be further described by the Parties in Part B of the Summary, as amended between the Participants from time to time. For the avoidance of doubt, any Controller to Controller Arrangements or Controller to Processor Arrangements which occur in connection with the Project, but are not described in Part B of the Summary, shall also be subject to this Framework and the Participants agree to:

5.3.1. take prompt steps to review and update Part B of the Summary; and

5.3.2. ensure Data Protection Legislation requirements for the arrangement are met, including but not limited to Article 26 UK GDPR and Article 28(3) UK GDPR as applicable.

5.4. The parties agree to only process Personal Data for the purpose of performance of the corresponding Project Activity and their obligations under the Project Terms of Reference (**Purpose**).

5.5. The parties shall not process Personal Data in a way that is incompatible with the Purpose.

6. **Duration of Processing**

6.1. Subject to clause 6.3, this Framework will remain in full force and effect so long as the Project Terms of Reference remains in effect (the **Term**).

6.2. Subject to clause 6.3, a Participant who exits from the Project Terms of Reference in accordance with [NOTE CLAUSE] shall also cease to be a party to this Framework when the applicable notice period expires.

6.3. Where a Participant retains any Personal Data in its possession or control, as Data Processor on behalf of another Participant under this Framework, following termination or exit in accordance with Clauses 6.1 and 6.2 above, the Framework shall continue to apply for any period of retention of that Personal Data.

7. **Framework Principles**

7.1. Each Participant agrees to adopt the following Framework Principles:

7.1.1. Take on, manage and account to the Participants for performance of the respective data roles and responsibilities set out in this Framework;

7.1.2. Communicate openly with SPoCs within the Framework about data sharing concerns, issues or opportunities arising from the Project;

7.1.3. Behave in a manner that gives full effect to this Framework;

7.1.4. Adhere to, and share with Participants where possible, statutory requirements and best practice in respect of the Project;

7.1.5. Recognise high-risk data processing under Project Activities and responsibilities/actions are of a time-critical nature;

7.1.6. Ensure sufficient and appropriately qualified resources are available and authorised to fulfil the responsibilities set out in this Framework; and

7.1.7. Act collaboratively and in good faith to support the Project and compliance with these Framework Principles.

8. **Key personnel**

8.1. Each Participant shall appoint an SPoC to act as their representative under the Framework. SPoCs must:

8.1.1. implement the Framework on behalf of the Participant within the Participant's body or organisation;

8.1.2. act as a single point of contact for Data Subject Right Requests arising out of the Project and such other statutory information requests;

8.1.3. work together to reach an agreement with regards to any issues arising from Framework; and

8.1.4. actively improve the effectiveness of the Framework.

9. **Compliance with Data Protection Legislation**

9.1. Each Participant must always ensure compliance with applicable Data Protection Legislation during the Term of this Framework.

9.2. Each Participant must at all times ensure it hold such valid registrations required by the Information Commissioner, unless an exemption applies.

9.3. For the avoidance of doubt:

9.3.1. Data Protection Legislation shall prevail over this Framework in the event of incompatibility; and

9.3.2. this Framework shall prevail over the Project Terms of Reference in the event of incompatibility.

10. **Data control**

10.1. The Participants' respective roles in relation to the Personal Data shall be described in Part B of the Summary.

11. **Controller to Controller Arrangement Obligations**

11.1. Where a Controller to Controller Arrangement arises between the Participants in respect of a Project Activity, the relevant Participants shall be subject to the obligations set out in Schedule 1 of this Framework.

12. **Controller to Processor Arrangement Obligations**

12.1. Where a Controller to Processor Arrangement arises between the Participants in respect of a Project Activity, the relevant Participants shall be subject to the obligations set out in Schedule 2 of this Framework.

13. **International Transfers**

13.1. A Participant may not make a transfer of Personal Data to a third party located outside the United Kingdom unless it:

13.1.1. is required by law to make the disclosure;

13.1.2. complies with the provisions of the Data Protection Legislation; and

13.1.3. ensures that;

13.1.3.1. the transfer is to a country approved under the applicable Data Protection Legislation as providing adequate protection; or

13.1.3.2. there are appropriate safeguards (such as IDTA's or UK Addendum to SCCs) or binding corporate rules in place in accordance with the Data Protection Legislation; or

13.1.3.3. the transferor otherwise complies with its obligations under the applicable Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; or

13.1.3.4. one of the derogations for specific situations in the applicable Data Protection Legislation applies to the transfer.

14. **Security and training**

14.1. The Participants each undertake to have in place appropriate technical and organisational security measures to:

14.1.1. prevent:

14.1.1.1. unauthorised or unlawful processing of the Personal Data; and

14.1.1.2. the accidental loss or destruction of, or damage to, the Personal Data

14.1.2. ensure a level of security appropriate to:

14.1.2.1. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and

14.1.2.2. the nature of the Personal Data to be protected.

14.2. The Participants shall keep such security measures under review and shall carry out any necessary updates as often as reasonably practicable.

14.3. Each Participant shall abide by any Access Restrictions described in Part B of the Summary.

14.4. Each Participant must ensure that its personnel are appropriately trained to handle and process the Personal Data in accordance with the Framework together with the applicable Data Protection Legislation and, where necessary, have entered into confidentiality agreements relating to the processing of Personal Data.

14.5. The level, content and regularity of training referred to in clause 14.2 shall be proportionate to the individual's role, responsibility and frequency with respect to their handling and processing of the Personal Data.

15. **Effect of non-compliance with Data Protection Legislation.**
Each Participant shall comply with all the obligations imposed on them under the Data Protection Legislation.

16. **Insurance**
The Participants shall at all times maintain in force adequate insurance policies with reputable insurance companies, against all risks that would normally be insured against by a prudent businessman in connection with the risks associated with this Framework.

17. **Indemnity**

17.1. The parties undertake to indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this Framework, except to the extent that any such liability is excluded under clause 19.

17.2. Indemnification hereunder is contingent upon:

17.2.1. the party(ies) to be indemnified (the indemnified party(ies)) promptly notifying the other party(ies) (the indemnifying party(ies)) of a claim,

17.2.2. the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and

17.2.3. the indemnified party(ies) providing reasonable co-operation and assistance to the indemnifying party(ies) in defence of such claim.

18. **Allocation of cost**
Each party shall perform its obligations under this Framework at its own cost.

19. **Limitation of Liability**
Limitation of Liability shall be as set out under the Project Terms of Reference.

20. **Dispute resolution under the framework**
In the event of a dispute relating to the Framework, the escalation procedure set out in the Project Terms of Reference shall be followed.

21. **Third party rights**
No one other than a Participant to this Framework, their successors and permitted assignees, shall have any right to enforce any of its terms.

22. **Variation**
No variation of this Framework shall be effective unless it is in writing and signed by all Participants (or their SPoCs).

23. **Waiver**
No failure or delay by a party to exercise any right or remedy provided under this Framework or by law shall constitute a waiver of that or any other right or

remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

24. **Severance**

24.1. If any provision or part-provision of this Framework is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Framework.

24.2. If any provision or part-provision of this Framework is deemed deleted under clause 24.1, the Participants shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

25. **Changes to the applicable law**

If Data Protection Legislation changes in a way that the Framework is no longer adequate for the purpose of governing lawful data sharing exercises, the Participants agree that the SPoCs will negotiate in good faith to review and, if required, vary the Framework in the light of the new legislation.

26. **Rights and remedies**

Except as expressly provided in this Framework, rights and remedies provided under this Framework are in addition to, and not exclusive of, any rights or remedies provided by law.

27. **Governing law**

This Framework and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

28. **Jurisdiction**

Each Participant irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with this Framework or its subject matter or formation.

29. **Interpretation**

The following definitions and rules of interpretation apply in this Framework.

Terms shown below in bold and throughout the Framework are defined terms for the purposes of interpretation and shall have the meaning set out below or as otherwise defined throughout the Framework.

| | |
|---|---|
| **Access Restrictions** | shall be the access restrictions to Personal Data corresponding to a Project Activity, as described in Part B of the Summary. |

| | |
|---|---|
| **Approved Sub-Processors** | shall be the sub-processors anticipated under the corresponding activity set out in Part B of the Summary. |
| **Project Activity** | shall mean the activities described in Part B of the Summary, each being distinct from one another, and severally governed by this Framework. |
| **Controller Receiver** | shall have the meaning given to it under 5.2.1. |
| **Controller to Controller Arrangement** | shall have the meaning given to it under 5.2.1. |
| **Controller to Processor Arrangement** | shall have the meaning given to it under 5.2.2. |
| **Criminal Offence Data** | shall mean Personal Data relating to criminal convictions and offences or related security measures to be read in accordance with section 11(2) of the DPA 2018 (and/or other applicable Data Protection Legislation). |
| **'Data Controller', 'Joint Controllers' 'Data Processor'** | shall have the meaning given to it by Data Protection Legislation. |
| **Data Protection Legislation** | means all applicable data protection and privacy legislation in force from time to time in the UK including but not limited to the UK GDPR; the Data Protection Act 2018 (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended. |
| **Data Subject** | means the identified or identifiable living individual to whom the Personal Data relates. |
| **Data Subject Rights** | means the Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to. automated individual decision-making in accordance with Data Protection Legislation. |
| **Domestic Law** | the laws of England and Wales. |
| **Framework or ISF** | this Framework together with any Schedules. |
| **Framework Principles** | shall mean the principles set out in clause 7. |

| | |
|---|---|
| **Information Commissioner or 'ICO'** | the Information Commissioner's Office or other such supervisory authority responsible for the enforcement of the Data Protection Legislation. |
| **Originating Controller** | shall mean:<br>a. in the case of a Controller to Controller Arrangement, the Participant disclosing the Personal Data to another Participant under the Framework; or<br>b. in the case of a Controller to Processor Arrangement, the Council, acting as either a data controller or data processor to a third-party, that instructs another Participant to act as Council Processor in respect of Personal Data;<br>and as further described in Part B of the Summary. |
| **Participants** | those parties described in clause 1.1 above. |
| **Permitted Recipients** | the parties to this Framework, the employees of each party, any third parties engaged by a Council in accordance with Schedule 1 Para 1.1(f) and(g) to perform obligations in connection with this Framework, and any other permitted recipients identified under the Summary or agreed between the parties in writing from time to time. For this avoidance of doubt, this shall not include sub-processor of Council Processors as such appointments are separately governed and defined. |
| **Personal Data** | shall mean the Personal Data and Special Categories of Personal Data and Criminal Offence Data to be shared by the Participants under each Project Activity, as set out in Part B of the Summary; and |
| **Personal Data Breach** | a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. |
| **Purpose** | shall have the meaning given to it under clause 5.4 of the Framework. |
| **Project Terms of Reference** | means the agreement between the Participants dated [ ]. |

| | |
|---|---|
| **Special Category Data, Processing**, **Supervisory Authority** and **appropriate technical and organisational measures** | as defined by the Data Protection Legislation. |
| **SPoCs** | shall be the individuals identified in the Part A of the Summary to represent each Participant in matters relating to this Framework unless otherwise agreed between the parties from time to time. |
| **Sub-Processor** | shall be the sub-processors identified in Part B of the Summary and those otherwise appointed in accordance with the process set out in Schedule 2. |
| **Subject Rights Request** | the exercise by a Data Subject of their rights under the Data Protection Legislation |
| **Term** | shall have the meaning given to it under clause 6.1 |
| **UK GDPR** | has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018. |

29.1. Clause, schedule and paragraph headings shall not affect the interpretation of this Framework.

29.2. Any Schedules form part of this Framework and shall have effect as if set out in full in the body of this Framework. Any reference to this Framework includes the Schedules.

29.3. Unless the context otherwise requires, words in the singular shall include the plural and, in the plural, shall include the singular.

29.4. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

29.5. A reference to legislation or a legislative provision shall include all subordinate legislation made from time to time under that legislation or legislative provision.

29.6. References to clauses and Schedules are to the clauses and Schedules of this Framework and references to paragraphs are to paragraphs of the relevant Schedule.

29.7. Any words following the terms including, include, in particular or for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

29.8. In the case of any ambiguity between any provision contained in the body of this Agreement and any provision contained in the Schedules or appendices, the provision in the body of this Framework shall take precedence.

29.9. A reference to writing or written includes email but not fax or any other instant or internet-based messaging platform.

29.10. Unless the context otherwise requires, reference to one gender shall include a reference to all genders.

## *Schedule 1 – Data Controller Obligations*

1.1 Any Data Controller under the Project, whether acting as an Originating Controller or Controller Receiver, shall:

(a) ensure that it has all necessary notices and consents and lawful bases in place to enable lawful transfer of the Personal Data to the Permitted Recipients for the Purposes;

(b) where necessary, ensure that it has and maintains an appropriate policy document relating to the Project Activities in accordance with Part 4 of Schedule 1 to the Data Protection Act 2018;

(c) give full information to any Data Subject whose Personal Data may be processed under this Framework of the nature of such processing. This includes giving notice that, on the termination of this Framework, Personal Data relating to them may be retained by or, as the case may be, transferred to one or more of the Permitted Recipients, their successors or assignees;

(d) process the Personal Data only for the Purposes;

(e) not disclose or allow access to the Personal Data to anyone other than the Permitted Recipients;

(f) ensure that all Permitted Recipients, excluding other Participants under this Framework, are subject to written contractual obligations concerning the Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this Framework;

(g) comply with Article 28 of the UK GDPR when appointing any Permitted Recipients, excluding other Participants under this Framework, and shall remain liable to the Originating Controller for the acts and omissions of the Permitted Recipient;

(h) inform any other Originating Controller or Controller Receiver of any actual or possible Personal Data Breach irrespective of whether there is a requirement to notify the Information Commissioner or Data Subject(s);

(i) work collaboratively with the any other Originating Controller or Controller Receiver (as applicable) to resolve and comply with its obligations to report a Personal Data Breach to the Information Commissioner and (where applicable) Data Subjects under Article 33 of the UK GDPR; and

(j) maintain appropriate data retention and deletion policies which ensure that it shall not retain or process Personal Data for longer than is necessary to carry out the Purpose(s).

1.2 **Mutual assistance.** Each Originating Controller and Controller Receiver under the Framework shall assist one another in complying with all applicable requirements of the Data Protection Legislation; as well as any applicable legal, regulatory and contractual responsibilities. In particular, they shall:

(a) consult with one another about any notices given to data subjects in relation to the Personal Data;

(b) promptly inform one another about the receipt of any Data Subject Rights request;

(c) not disclose, release, amend, delete or block any Personal Data in response to a Data Subject Rights Request without first consulting one another wherever possible;

(d) assist one another without cost in responding to any request from a Data Subject and in ensuring compliance with their obligations under the Data Protection Legislation with respect to security, Personal Data Breach notifications, data protection impact assessments and consultations with the Information Commissioner or other regulators;

(e) provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner;

(f) notify one another without undue delay on becoming aware of any breach of the Data Protection Legislation;

(g) use compatible technology for the processing of Personal Data to ensure that there is no lack of accuracy resulting from Personal Data transfers;

(h) maintain complete and accurate records and information to demonstrate its compliance with this Framework and allow for audits by the other party/parties or the other parties' designated auditor; and

(i) contact the SPoC for all issues arising out of the Data Protection Legislation, including the joint training of Permitted Recipients, the procedures to be followed in the event of a Personal Data Breach, and the regular review of the parties' compliance with the Data Protection Legislation.

1.3 Where the parties are Joint Controllers of Personal Data:

(a) the joint arrangements between the Joint Controllers shall be as set out in Part B or as otherwise agreed between the parties from time to time; and

(b) they must comply with their obligations under Article 26 of the UK GDPR and:

(i) shall not use the jointly controlled Personal Data for any independent purpose;

(ii) shall make available to Data Subjects the essence of the arrangements contemplated between the Joint Controllers;

(iii) acknowledge that Data Subjects may exercise their rights under the Data Protection Legislation in respect of and against each Joint Controller in accordance with Article 26(3) of the UK; and

(iv) agrees to provide any Joint Controller such cooperation as may reasonably be required to assist that Joint Controller to comply with its obligations under Article 26 of the UK GDPR;

(c) each Joint Controller is jointly responsible and is jointly accountable for compliance with the Data Protection Legislation and for ensuring compliance with this Framework.

***Schedule 2 – Data Processing Obligations***

1.1 Where an Originating Controller instructs another Participant to act as its data processor of Personal Data in respect of a Project Activity (**Council Processor**), the parties acknowledge:

(a) in accordance with Article 28(3) UK GDPR, Part B of the Summary to this Framework describes the subject matter, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Council Processor may process the Personal Data to fulfil the Purposes; and

(b) the Originating Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Council Processor.

1.2 Without prejudice to the generality of clause 9 of this Framework, the Originating Controller will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Council Processor and/or lawful collection of Personal Data by the Council Processor under this Framework.

1.3 Where a Participant is instructed by an Originating Controller to act as its Council Processor, and in addition to the requirements under the Framework, it must:

(a) only process Personal Data to the extent, and in such a manner, as is necessary for the to fulfil the Purpose and in accordance with the Originating Controller's written instructions. The Council Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Framework or the Data Protection Legislation. The Council Processor must promptly notify the Originating Controller if, in its opinion, instructions do not comply with the Data Protection Legislation;

(b) not transfer any Personal Data outside of the UK unless the prior written consent of the Originating Controller has been obtained and the requirements of clause 13 of the Framework is met;

(c) assist the Originating Controller, at the Originating Controller's cost, in responding to any Data Subject Request and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(d) notify the Originating Controller without undue delay on becoming aware of a Personal Data Breach;

(e) comply promptly with any Originating Controller's instructions to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing;

(f) maintain the confidentiality of the Personal Data and not disclose the Personal Data to third parties unless the Framework specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Information Commissioner). If a Domestic Law, court or regulator (including the Information Commissioner) requires the Council Processor to process or disclose the Personal Data to a third party, the Council Processor must first inform the Originating Controller of such legal or regulatory requirement and give the Originating Controller an opportunity to object or challenge the requirement, unless the Domestic Law prohibits the giving of such notice;

(g) reasonably assist the Originating Controller with meeting the Originating Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Council Processor's processing and the information available to the Council Processor, including in relation to Data Subject Rights, data protection impact assessments, and reporting to and consulting with the Information Commissioner under the Data Protection Legislation;

(h) not disclose the Personal Data to any Data Subject or to a third party other than at the Originating Controller's request or instruction, as provided for by this Framework or as required by law;

(i) inform the Originating Controller if it receives a Subject Rights Request relating to the Personal Data as soon as possible (and in any event, no later than 5 working days following receipt of the request);

(j) taking into account the nature of the Council Processor's processing and the information available to the Council Processor, reasonably assist the Originating Controller with meeting the Originating Controller's legal and contractual responsibilities as a Public Authority.

(k) maintain complete and accurate records and information to demonstrate its compliance with this clause and allow for audits by the Originating Controller or the Originating Controller's designated auditor.

(l) at the written direction of the Originating Controller, delete or return Personal Data (limited to the data which is subject to the processing arrangement) and copies thereof to the Originating Controller on termination of the agreement unless required by Domestic Law to store Personal Data.

1.4 A Council Processor will:

(a) immediately and in any event without undue delay notify the Originating Controller in writing if it becomes aware of:

(i) the loss, unintended destruction or damage, corruption, or unuseability of part or all of the Personal Data. The Council Processor will restore such Personal Data at its own expense as soon as possible.

(ii) any accidental, unauthorised or unlawful processing of the Personal Data; and/or

(iii) any Personal Data Breach.

(b) upon becoming aware of (i) (ii) (iii) above and without undue delay, provide the Originating Controller with the following written information:

(i) description of the nature of (i), (ii) and/or (iii), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(ii) the likely consequences; and

(iii) a description of the measures taken or proposed to be taken to address (i), (ii) and/or (iii), including measures to mitigate its possible adverse effects.

(c) reasonably co-operate with the Originating Controller at no additional cost to the Originating Controller, in the Originating Controller's handling of any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, including but not limited to:

(i) assisting with any investigation;

(ii) providing the Originating Controller with physical access to any facilities and operations affected;

(iii) facilitating interviews with the Council Processor's employees, former employees and others involved in the matter;

(iv) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Originating Controller; and

(v) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

(d) not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data

Breach without first obtaining the Originating Controller's written consent, except when required to do so by Data Protection Legislation.

1.5 The Council Processor agrees that the Originating Controller has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Information Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Originating Controller's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

1.6 The Originating Controller hereby consents to the Council Processor appointing the Anticipated Sub-Processors as third-party processors of Personal Data under this Framework. The Council Processor confirms that it has entered or (as the case may be) will enter with the third party processor into a written agreement incorporating terms which are substantially similar to those set out in this Schedule 2 and in either case which the Council Processor confirms reflect and will continue to reflect the requirements of the Data Protection Legislation, in particular Article 28 of the UK GDPR. As between the Originating Controller and the Council Processor, the Council Processor shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this paragraph 1.6 of Schedule 2.

# Redruth Town Council
# Legitimate Interests Assessment (Template)

Udated October 2026

| **Document Controls** | |
|---|---|
| **Owner:** | Data Protection Officer |
| **Reviewed by:** | Full Council |

| **Date** | **Initials** | **Revisions made** |
|---|---|---|
| October 2026 | | DRAFT |

If you have any queries or suggested amendments to this document, please contact the Owner named above. Please archive all historic versions of this notice for audit

## WHAT IS A LEGITIMATE INTEREST ASSESSMENT?

A Legitimate Interests Assessment assists a controller in demonstrating that reliance on Article 6(1)(f) UK GDPR is appropriate, necessary and balanced against the rights and freedoms of data subjects.

Please note: Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

## HOW TO COMPLETE A DATA PROTECTION IMPACT ASSESSMENT (DPIA)

**Step 1: Complete Identifying Details and Description of Activity.**

**Step 2: Part A: Purpose Test**

**Part B: Necessity Test**

**Part C: Balancing Test**

**Step 3: Complete the Risk to Rights and Freedoms Assessment.** This table enables the asses to meet the requirements of Article 35 (7) (c) UK GDPR and Section 64 Data Protection Act 2018 by identifying the origin, nature, particularity and severity of the risks presented by the activity. For each risk potential impacts and threats are identified, together with the likelihood and severity of those risks and threats, and any measures envisaged to treat those risks are determined (as required by Article 35(7)(d) UK GDPR).

**Step 4: Outcome and Approval.** This section aims to record the outcome of the assessment, together with decision details, decision maker details, quality control data and any review requirements. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

**LEGITIMATE IMPACT ASSESSMENT**

Title of processing activity:

*Ref.*

[DATE]

## IDENTIFYING DETAILS

| | |
|---|---|
| Controller Name | |
| Brief description of activity | |
| Categories of affected data subject? | |
| Are any of these data subjects not already known to the business (i.e members of the public) | |
| What is the nature of the data to be processed? | |
| Is this likely to form part of your Public Task? | If yes, LI not suitable. |
| How will the business obtain the personal data relating to the affected data subject? | |
| *[Any other details, as practicable]* | |

## STEP 2: PART A: PURPOSE TEST

| | *Explanation* |
|---|---|
| **Context** of activity | |
| **Purpose** of activity | |
| What **Legitimate Interest** is being pursued | |
| What would the impact be if you couldn't go ahead? | |
| Would your use of the data be unethical or unlawful in any way? | |
| **Benefits** of activity for individuals, including data subjects | |

| | | |
|---|---|---|
| | for the data controller | |
| | for the society as a whole | |
| **Drawbacks of activity** | for individuals, including data subjects | |
| | for the data controller | |
| | for the society as a whole | |
| Are you complying with any specific data protection rules or any other laws or industry guidelines or codes of practice. | | |

## PART B: NECESSITY TEST

| | | |
|---|---|---|
| **Will processing actually help to achieve the purposes?** | | |
| **Is processing proportionate?** | | |
| **Measures:** | | |
| | Have similar or less intrusive activities been considered or attempted? | |
| | How does the proposed activity achieve the Purpose outlined under Stage 1 above? | |
| | How will personal data be limited to the activity only | |

| | | |
|---|---|---|
| | (avoiding function creep?) | |
| | How will you support data subject rights? | |
| | How will you inform stakeholders that you are conducting this activity? Is it appropriate to consult with Data Subjects and their representatives? | |
| | What measures are taken to ensure that processors comply? | |
| | How are international transfers safeguarded (if applicable) | |

**PART C: Balancing Test**

| | | |
|---|---|---|
| **Recognised Legitimate Interest applies?** | public task disclosure request condition | |
| | national security, public security and defence condition | |
| | emergencies condition | |
| | crime condition | |

| | | | |
|---|---|---|---|
| | safeguarding condition | | |
| Does the activity relate to **special category data or criminal conviction data**? | | | IF YES, LEGITIMATE INTERESTS CAN BE USED. HOWEVER, YOU NEED TO APPLY SPECIAL CATEGORY / CRIMINAL OFFENCE CONDITIONS UNDER DATA PROTECTION ACT 2018. |
| Do the affected data subjects include **children or vulnerable adults**? | | | IF YES, LEGITIMATE INTERESTS CAN BE USED. HOWEVER, YOU NEED TO GIVE EXTRA WEIGHT TO THEIR INTERESTS AND YOU NEED A MORE COMPELLING INTEREST TO JUSTIFY ANY POTENTIAL IMPACT ON CHILDREN ON THIS BASIS. |
| **Reasonable expectations of the Data Subject** | Would the individual expect the activity? | | |
| | Is information considered private and confidential? | | |
| | Would they object if given the chance? | | |
| | Does the data contain information | | |

| | | |
|---|---|---|
| | regarding personal or professional capacity? | |
| **Potential Impacts of Activity** | | |
| **Safeguards** | Opt Out? | |
| | Additional privacy messaging? | |
| | Other? | |
| **DPO / SPO Advice (if required)** | | |

**STEP 6: OUTCOME**

| OUTCOME | |
|---|---|
| PENDING | |
| Legitimate Interest Proven | |
| Legitimate Interest Failed | |
| **DECISION DETAIL** | |
| *Please insert reasons and/or requirements* | |
| *Privacy Information Updated to account for activity?* | *YES [ ] date:*<br>*No [EXPLAIN REASON]* |
| **OUTCOME REVIEW REQUIREMENTS** | |
| How often will you conduct a **review** of this activity to ensure it is still required? | [Annually] |

| ***Completed by:*** | | ***Authorised By:*** |
|---|---|---|
| Name: | | |
| Role: | | |
| Date: | | |
| Signed: | | |

**REDRUTH TOWN COUNCIL**

**REPORT FOR: Meeting of Full Council on Monday 30th November 2026**

**SUBJECT OF REPORT: Town Clerk's Report**

## SUMMARY OF IMPLICATIONS

a. Policy Yes
b. Financial Yes
c. Legal Yes

## 1.0 TERMS OF REFERENCE

To report on progress during the period.

## 2.0 REPORT

2.1 Below is a table of actions on existing and new items, some of which were reported in the last Full Council meeting and the progress that has been made since the last Full Council meeting in October 2026.

| **Agenda Item number:** | **Issue:** | **Action taken by Town Clerk or / for decision:** |
|---|---|---|
| Existing item | Devolution of Victoria Park and Trefusis Park | Since the last meeting, Cornwall Council's devolution team have responded on the matter of the equipment as discussed. Their response is below.<br><br>*Cormac procured 'cut and collect' meadow mowers e.g. Grillo and Amazone Profihopper to manage some wildflower verges & incidental areas, as well as Green Infrastructure for Growth and Making Space for Nature sites. Projects were delivered in 17 towns on approx. 75 sites.*<br>*Mowers were bought for large geographic areas – for west, mid and east Cornwall. The mowers used in Redruth can also be used in Camborne, Carn Brea, St Day, Carharrack, Penzance etc and not just for one or two sites specifically. RTC may choose to commission Cormac to support their cutting programme (labour & machinery), but the loan of equipment only is not a feasible* |

| | | |
|---|---|---|
| | | *proposal. It would create so many issues around safety and liability, as well as maintenance standards/use, to make an arrangement unviable.*<br><br>**For decision:**<br>In light of the fact that the Council is currently drafting the budget requirements for 2027/28, the final offer from Cornwall Council is £75k for the devolution of three parks, Victoria, Trefusis and Treskerby.<br><br>The Council needs to debate this and decide on whether to proceed or not with the devolution of these assets. If the Council decides to proceed, I recommend moving the detail of the transfers to the Asset Management Committee. |
| New item | Anti-social Behaviour | The new ASB Caseworker has settled in extremely well and is building good relationships with the team and stakeholders, with surgeries planned in the library.<br>There will be a presentation at the December Full Council meeting. |
| Existing item | New website | The Council's new website has launched and already there has been some positive feedback.<br><br>If you have not already had chance to, please do have a browse and share with your networks.<br><br>There is still some work on Accessibility to do but this is all in hand with the web developer and the Communications Manager and updates are on the site statement. |
| New item | Calendar of dates | Please find attached the revised Calendar of dates, the Annual Town Meeting is scheduled for 2027 to take place on 13th May 2027. |
| New item | Data Protection | This month, I have been dealing with an increase in the number of Freedom of Information requests and Subject Access Requests. |
| New item | Highways issues | This month I have escalated a number of Highways related matters to Cornwall Councillors and the Highways department for action, some of these are persistent issues. |
| New item | Remembrance Day | I would like to thank all those who attended or helped organise the Remembrance events throughout the parish. |

| | | |
|---|---|---|
| | | The continued partnership with the Royal British Legion is very important to the community. |
| New item | Fundraiser | The fundraiser for independent businesses affected recently with broken windows raised a total of £777.45 which will be split equally and distributed between the businesses. Thank you to all those who donated. |

## 3.0 RECOMMENDATIONS

To note and accept the report of the Town Clerk.

# Redruth Town Council
## Calendar of Council, Committee Meetings and Event Dates 2027-2028

| | Apr'27 | May'27 | Jun'27 | Jul'27 | Aug'27 | Sep'27 | Oct'27 | Nov'27 | Dec'27 | Jan'28 | Feb'28 | Mar 28 | Apr'28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Annual Meeting | | 10 | | | | | | | | | | | |
| Full Council | 26 | 24 | 28 | 26 | | 27 | 25 | 29 | 20 | 31 | 28 | 27 | 24 |
| Asset Management Committee | | | 7 | | | 6 | | | 6 | | | 6 | |
| Community Committee | | 17 | | | 9 | | | | 13 | | | | 3 |
| Staffing Committee | 19 | | | 19 | | | 18 | | | 17 | | | 10 |
| Finance Committee | 19 | | | 19 | | | 18 | | | 17 | | | 10 |
| Planning Committee | 26 | 24 | 7 | 26 | 9 | 27 | 25 | 29 | 6 | 31 | 28 | 27 | 3 |
| Annual Town Meeting | | 13 | | | | | | | | | | | |
| Local Heroes' Awards | | | | | | | 8 | | | | | | |
| St. Piran's Day Festival | | | | | | | | | | | | 4 | |
| Murdoch Day | | | 12 | | | | | | | | | | |
| Youth Fest | | | | 31 | | | | | | | | | |
| Victoria Park Fun Day | | | | 10 | | | | | | | | | |
| International Pasty & Mining Festival | | | | | | 10/11/12 | | | | | | | |
| Remembrance Sunday | | | | | | | | 14 | | | | | |
| Redruth in Lights | | | | | | | | | 4 | | | | |
| Grotto | | | | | | | | | 4 & 11 | | | | |

**NB: Planning & Staffing Committees will always commence at 6pm**

**Payment Report** **Full Council Meeting: 30 November 2026**
**Redruth Town Council**
**For the period 20 October 2026 to 27 November 2026**

| Date | Description | Payment inc VAT | |
|---|---|---|---|
| **Credit card** | | | |
| 20 Oct 2026 | Seton | 49.12 | Flood barriers |
| 25 Oct 2026 | Mailchimp | 41.99 | Subscription |
| 26 Oct 2026 | Eventbrite | 11.55 | Sales training fee - Business Liaison Manager |
| 26 Oct 2026 | Eventbrite | 11.55 | Sales event fee - Business Liaison Manager |
| 28 Oct 2026 | BHGS Ltd | 491.80 | Equipment and materials for polyunnel |
| 28 Oct 2026 | BHGS Ltd | 42.83 | Equipment and materials for polytunnel |
| 02 Nov 2026 | Lloyds Bank credit card | 3.00 | Monthly Bank fee |
| 04 Nov 2026 | Brevo | 140.00 | Subscription |
| 04 Nov 2026 | Etheringtons Pasties | 150.00 | Pasties for Remembrance Sunday |
| 12 Nov 2026 | Arch Cafe | 89.15 | Town meeting refreshments |
| 16 Nov 2026 | Land Registry | 14.00 | Property searches - Trewirgie Fields |
| 18 Nov 2026 | Kingfisher Direct Limited | 139.10 | Cable protector for Christmas tree |
| **Total Credit card** | | **£ 1,184.09** | |
| **Current Account** | | | |
| 16 Oct 2026 | Sage DD | 217.80 | Payroll software |
| 16 Oct 2026 | Control Print Limited | 871.00 | Redruth Record printing |
| 19 Oct 2026 | Thirsty Work Ltd DD | 33.00 | Water cooler |
| 19 Oct 2026 | British Gas 604218508 Civic elec | 2,292.52 | Electricity - Civic Centre |
| 19 Oct 2026 | British Gas 604218559 5MW | 41.91 | Electricity - 5 MW |
| 19 Oct 2026 | British Gas 604218560 4MW | 21.44 | Electricity - 4MW |
| 19 Oct 2026 | British Gas 604218583 3MW | 9.73 | Electricity - 3MW |
| 19 Oct 2026 | British Gas 604218584 11-12MW | 78.46 | Electricity - 11MW |
| 19 Oct 2026 | British Gas 604218585 6MW | 6.93 | Electricity - 6MW |
| 20 Oct 2026 | British Gas 603225849 Facilities Yard | 34.24 | Electricity - Facilities Yard |
| 21 Oct 2026 | HMRC PAYE and NI | 29,219.54 | PAYE/NI payment for September 2026 |
| 21 Oct 2026 | Adobe Systems Software | 175.99 | Adobe software |
| 21 Oct 2026 | Safepoint | 71.76 | Lone worker protection |
| 21 Oct 2026 | Spotify | 17.99 | Spotify payment for event |
| 22 Oct 2026 | Xero (UK) Ltd | 46.80 | Finance software |
| 22 Oct 2026 | Imagin | 35.52 | Photo ID badges |
| 23 Oct 2026 | Next Level Lifts Ltd | 363.60 | Lift sservice - Chambers and Civic Centre |
| 23 Oct 2026 | British Gas 604218351 Market Hall | 459.94 | Electricity - Market Hall |
| 23 Oct 2026 | Bunzl Cleaning & Hygiene Supplies | 175.19 | Cleaning materials |
| 23 Oct 2026 | Lamps & Tubes Illuminations Ltd | 8,509.20 | Christmas Lights purchase |
| 23 Oct 2026 | Roscoe Communications | 2,400.00 | Copywriting for website |

| | | | |
|---|---|---|---|
| 23 Oct 2026 | Nick Ferris Skip Hire | 468.00 | Skip - Facilities Yard |
| 23 Oct 2026 | C Applegarth Cleaning Services | 45.00 | Sign cleaning |
| 23 Oct 2026 | P J D Martin Ltd | 340.68 | Remove kitchen area from office |
| 23 Oct 2026 | Office Smart | 7.84 | Stationery |
| 23 Oct 2026 | Cornwall Electrical Contractors Ltd | 439.20 | Repairs to stairwell lights - Chambers |
| 23 Oct 2026 | Cornwall Fabrication | 105.60 | Supply traingular plate for Facilities yard |
| 23 Oct 2026 | Source 4 Business 2147244101 | 286.28 | Water rates - Chambers |
| 23 Oct 2026 | Cornwall College Group | 1,600.00 | College course - Facilities Manager |
| 23 Oct 2026 | Royal Mail | 177.48 | Stamps for Library |
| 23 Oct 2026 | Core Highways | 3,129.24 | Traffic management for Remembrance Sunday |
| 26 Oct 2026 | Vodafone | 115.70 | Mobile phones |
| 26 Oct 2026 | British Gas 604218451 Civic Gas | 28.01 | Gas bill - Civic Centre |
| 27 Oct 2026 | British Gas 604218558 New Cut | 34.99 | Electricity - New Cut |
| 27 Oct 2026 | British Gas 604218561 Public Mural | 23.12 | Electricity - Public Mural |
| 27 Oct 2026 | British Gas 604218582 St Rumons | 16.51 | Electricity - St Rumons |
| 27 Oct 2026 | British Gas 604218586 Elec Chambers | 550.39 | Electricity - Chambers |
| 29 Oct 2026 | Details with-held for data protection | 60,416.55 | Net salaries October 2026 |
| 29 Oct 2026 | Information Commissioners Office | 73.00 | ICO subscription |
| 30 Oct 2026 | Acronyms Limited DD | 3,071.90 | IT support, leased line, MS software |
| 30 Oct 2026 | Health Assured | 109.99 | Employee Assistance programme |
| 31 Oct 2026 | Unity Trust Bank | 35.65 | Bank charges |
| 02 Nov 2026 | Biffa R39515*1*1 MW | 527.47 | Waste disposal |
| 02 Nov 2026 | Cornwall Council 802658743 | 165.00 | Business rates |
| 02 Nov 2026 | Cornwall Council 802804557 | 239.00 | Business rates |
| 02 Nov 2026 | Cornwall Council 803069656 | 219.00 | Business rates |
| 02 Nov 2026 | Cornwall Council 802772285 | 3,036.00 | Business rates - Civic Centre |
| 02 Nov 2026 | Cornwall Council 800297361 | 917.00 | Business rates - Chambers |
| 02 Nov 2026 | Biffa R36029 | 124.14 | Waste disposal |
| 02 Nov 2026 | Biffa R36029 | 68.06 | Waste disposal |
| 02 Nov 2026 | Biffa R36029 | 197.10 | Waste disposal |
| 02 Nov 2026 | Biffa R36029 | 68.06 | Waste disposal |
| 02 Nov 2026 | South West Water 10721248 St Rumons | 12.94 | Water - St Rumons |
| 02 Nov 2026 | PWLB | 7,868.58 | Loan repayment - Civic Centre |
| 03 Nov 2026 | Xerox Finance Ltd | 324.72 | Photocopier lease |
| 04 Nov 2026 | Hewlett Packard | 276.63 | Councillors tablets |
| 09 Nov 2026 | Acronyms Limited DD | 355.55 | VOIP office phones |
| 09 Nov 2026 | UK Fuels Limited | 7.20 | Fuel charge |
| 13 Nov 2026 | Tregothnan | 335.00 | Christmas tree for Town Centre |
| 13 Nov 2026 | Source 4 Business 5019325201 | 9.47 | Water rates - Raymond Road allotments |
| 13 Nov 2026 | Office Smart | 136.18 | Stationery |
| 13 Nov 2026 | Krowji | 183.75 | Rent - Facilities Yard |
| 13 Nov 2026 | Cornwall Lifeskills | 465.00 | First Aid and Bleed Management training |
| 13 Nov 2026 | Cornwall Fabrication | 120.00 | Repair gate for Plain an Gwarry |
| 13 Nov 2026 | Cornwall Pension Fund | 19,401.32 | Pension contributions - October 26 |

| | | | |
|---|---|---|---|
| 13 Nov 2026 | MacSalvors | 238.91 | Tools, equipment and PPE - Facilities team |
| 13 Nov 2026 | Scientific Services Ltd | 330.00 | Legionella testing |
| 13 Nov 2026 | Truro Tractors | 180.88 | Machinery repairs |
| 13 Nov 2026 | Go Displays | 350.36 | Mobile folding display boards |
| 13 Nov 2026 | Warrior Warehouses | 64.00 | Refuse sacks |
| 13 Nov 2026 | The Green Waste Company | 26.00 | Green waste disposal |
| 13 Nov 2026 | Stephens Scown LLP | 2,182.20 | General employment advice |
| 13 Nov 2026 | Starboard Systems Limited | 489.60 | Civic.ly subscription |
| 13 Nov 2026 | South West Hygiene | 130.66 | Dust mats, sanitary bins |
| 13 Nov 2026 | SLCC | 505.00 | Conference fee |
| 13 Nov 2026 | Scorrier House | 720.00 | Staff training day |
| 13 Nov 2026 | Roscoe Communications | 2,400.00 | Working on Comms Strategy, Marketing Campaign toolkit |
| 13 Nov 2026 | P J D Martin Ltd | 238.45 | Repairs to toilet in Civic Centre |
| 13 Nov 2026 | Peake (GB) Limited | 42.00 | Removal of deer carcass |
| 13 Nov 2026 | Nathan Heyes | 40.00 | SWRLS workshop |
| 13 Nov 2026 | NALC | 336.00 | Delegate ticket - study tour 2027 |
| 13 Nov 2026 | Mill Signs | 132.00 | Floral display signs |
| 13 Nov 2026 | Gregzilla | 550.00 | Removal of bunting from Town Centre |
| 13 Nov 2026 | DR Building Materials | 112.49 | Materials for Facilities Team |
| 13 Nov 2026 | Creative Kernow Ltd | 276.00 | Advert in Cornwall 365 |
| 13 Nov 2026 | Corserv Solutions Ltd t/a Cormac Solutions | 2,419.94 | Vehicle lease costs |
| 13 Nov 2026 | Cornwall Council | 35.50 | Mental Health First Aid training |
| 13 Nov 2026 | C Applegarth Cleaning Services | 25.00 | Window cleaning |
| 13 Nov 2026 | Bunzl Cleaning & Hygiene Supplies | 252.36 | Cleaning materials |
| 13 Nov 2026 | Aquam Water Services Ltd | 211.20 | Standpipe hire |
| 13 Nov 2026 | Annie Kitto | 2,225.00 | Cleaning of public toilets |
| 13 Nov 2026 | Alliance Tool Hire (South West) | 1,213.56 | Dehumidifier hire |
| 13 Nov 2026 | HMRC PAYE and NI | 21,400.26 | PAYE and NIC October 26 |
| 13 Nov 2026 | Cornwall Electrical Contractors Ltd | 16,780.78 | Electrical works, road closure, traffic management, installation Christmas lights |
| 13 Nov 2026 | First Aid For Less | 532.74 | First Aid box supplies |
| 13 Nov 2026 | Fox Security & Training Ltd | 2,030.40 | Temporary staff |
| 13 Nov 2026 | MacSalvors | 165.50 | Tools, equipment and PPE - Facilities team |
| 13 Nov 2026 | Scientific Services Ltd | 330.00 | Legionella testing |
| 13 Nov 2026 | Truro Tractors | 1,444.31 | Purchase of chainsaws and equipment |
| 13 Nov 2026 | Wicksteed Leisure Ltd | 100,000.00 | 1st instalment - play equipment East End |
| 16 Nov 2026 | Opie Oils - DD | 233.05 | Machinery fuel |
| 16 Nov 2026 | UK Fuels Limited | 145.45 | Vehicle fuel |
| 16 Nov 2026 | Wicksteed Leisure Ltd | 58,613.05 | 2nd instalment - East End plus PnG roundabout |
| 17 Nov 2026 | British Gas 604218448 7MW | 23.10 | Electricity - 7MW |
| 17 Nov 2026 | British Gas 604218508 Civic elec | 2,774.82 | Electricity - Civic Centre |
| 17 Nov 2026 | British Gas 604218584 11-12MW | 15.74 | Electricity - 12MW |
| 17 Nov 2026 | PLAN.COM DD ACCOUN | 1,284.00 | Mobile phones |
| 18 Nov 2026 | Thirsty Work Ltd DD | 33.00 | Water cooler |
| 18 Nov 2026 | British Gas 603225849 Facilities Yard | 34.70 | Electricity - Facilities Yard |

| | | | |
|---|---|---|---|
| 18 Nov 2026 | 1st Office Equipment Ltd | 869.94 | Photocopier lease |
| 19 Nov 2026 | Adobe Systems Software | 175.99 | Adobe subscription |
| 19 Nov 2026 | British Gas 604218560 4MW | 24.24 | Electricity - 4MW |
| 20 Nov 2026 | Safepoint | 71.76 | Lone worker security |
| 23 Nov 2026 | UK Fuels Limited | 138.33 | Vehicle fuel |
| 27 Nov 2026 | Details with-held for data protection | 70,762.21 | Net salaries November 2026 |

| | |
|---|---|
| **Total Current Account** | **444,825.34** |

**Petty Cash**

| | | | |
|---|---|---|---|
| 26 Oct 2026 | B&M | 5.99 | Coffee |
| 26 Oct 2026 | B&M | 5.99 | Coffee |
| 02 Nov 2026 | Taxi | 44.00 | Taxi for staff member home from hospital |
| 05 Nov 2026 | Library | 20.00 | Return of float |
| 05 Nov 2026 | Specsavers | 25.00 | Eye test - staff member |
| 09 Nov 2026 | Iceland | 10.25 | Coffee, tea etc for Facilities Yard |
| 09 Nov 2026 | Iceland | 16.75 | Tea, coffee |
| 09 Nov 2026 | Poundland | 2.00 | Container for Youth Council stall |
| 09 Nov 2026 | Tesco | 6.15 | Items for Youth Council stall |
| 09 Nov 2026 | Poundland | 10.00 | Items for Youth Council stall |
| 10 Nov 2026 | Iceland | 13.00 | Coffee |
| 12 Nov 2026 | Boots UK Ltd | 9.50 | Covid tests for office |
| 18 Nov 2026 | Iceland | 6.50 | Coffee |
| 18 Nov 2026 | Iceland | 12.50 | Coffee |
| 18 Nov 2026 | Country Store Health Foods | 2.49 | Oat milk |
| 19 Nov 2026 | Green News and Food | 2.30 | Milk |
| 19 Nov 2026 | Jims | 1.49 | Petty cash book |
| 20 Nov 2026 | Green News and Food | 4.99 | Batteries |
| 23 Nov 2026 | Max Spielmann | 12.00 | Picture frames |
| 23 Nov 2026 | Cash Generator | 10.00 | 64gb USB stck |
| 24 Nov 2026 | Specsavers | 25.00 | Eye test - staff member |

| | |
|---|---|
| **Total Petty Cash** | **245.90** |