Redruth Town Council
Information Technology (IT) Policy

Updated October 2026

Document Controls	
Owner:	Town Clerk
Reviewed by:	Full Council

Date	**Initials**	**Revisions made**
October 2026	Chairman – Redruth Town Council	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

1. Introduction

1.1 Redruth Town Council (the Council) recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

1.2 This policy should be read in conjunction with the Council's adopted:

- Staff Handbook (Staff Only)

The public policies are available at the Town Council's website using the following link: www.redruth-tc.gov.uk

1.3 The Council's IT provider is Acronyms IT: https://www.acronyms.co.uk/

2. Aim

2.1 The purpose of this IT policy is to establish clear parameters for how Councillors (Members), staff and other authorised users use council-provided technology or equipment in the course of their duties including:

- Expectations for appropriate use of equipment and systems.
- Awareness of risks associated with IT use.
- Safeguarding the council's data and digital assets.
- Clarification on what constitutes acceptable and unacceptable use.
- Defines the consequences of policy breaches.

3. Scope

3.1 This policy applies to all Councillors, staff and other authorised users, regardless of their working location or pattern, including those who are office-based, or work on a flexible or part-time basis. It sets out expectations for the appropriate use of IT equipment and systems provided by the Council.

4. Monitoring of IT Use

4.1 As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so, and Councillors, employees and other authorised users are informed that such monitoring may take place.

4.2 Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

4.3 Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

5. Computer use

5.1 Hardware

5.1.1 Council computer equipment is provided for council purposes; however

reasonable personal use is permitted (reasonable interpreted as in the opinion of the Town Clerk or Deputy Town Clerk). Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff and other authorised users are asked to restrict any personal use to official lunch breaks, before or after working hours or outside of official council meetings.

5.1.2 All councillors, staff, and other authorised users must lock their devices when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

5.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

5.1.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

5.1.5 All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

5.1.6 Equipment should not be dismantled or reassembled without seeking advice.

5.1.7 Councillors, staff and other authorised users are not to purchase any computer or mobile equipment (including software) unless previously authorised.

5.1.8 Personal disks, USB stick, CDs, DVDs, data storage devices etc. cannot be used on council computers without the prior approval of the Clerk or Council.

5.1.9 The council connects to a number of authorised wireless networks. Using a portable device to make personal Wi-Fi hot spots which bypass existing Wi-Fi is not allowed.

5.1.10 Any faults or necessary repairs must be reported to the Clerk in the first instance, or to the Council's IT provider.

5.1.11 All users must only access Council systems using their own allocated username and password. Users must not use another person's login credentials or permit another person to access Council systems using their credentials.

5.1.12 Staff must log out and shut down their computers at the end of each working day, unless otherwise authorised or instructed by the Council's

IT provider.

5.1.13 Users must not delete, destroy or modify existing systems, programmes, information or data, except where authorised in the proper performance of their duties.

5.1.14 Software must not be downloaded or installed from external sources, and devices or equipment, including mobile phones, tablets and USB storage devices, must not be connected to Council systems without prior authorisation from the Council's external IT provider, Acronyms.

6. Equipment

6.1 Portable Equipment

6.1.1 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

6.1.2 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home.

6.1.3 Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

6.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

6.1.5 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods-for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

6.1.6 All users must report suspected cyber incidents immediately to the Clerk and the Council's IT provider.

6.1.7 If an item of portable equipment is lost or damaged this should be reported to the clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first

£250 of the loss/damage.

6.1.8 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken in council offices, without the prior written permission of the clerk. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

6.1.9 Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

6.1.10 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the clerk.

6.2 Mobile phones

6.2.1 Mobile telephones issued by the Council remain the property of Redruth Town Council and must be returned when employment ends or a Councillor ends their term in office or when requested by the Council .

6.2.2 Employees must not use Council-issued mobile telephones whilst driving. Where a call is necessary, the driver must first stop in a safe and lawful location before making or receiving the call.

6.2.3 Employees and Councillors using mobile telephones whilst carrying out Council duties must comply with road traffic legislation and the Council's applicable mobile telephone procedures.

7. Use of own devices

7.1 The Council does not permit the use of own devices, unless in exceptional circumstances which are preauthorised by the Town Clerk or Deputy Town Clerk.

7.2 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). For Workers or Contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

7.3 In cases of legal proceedings against the council, it may be necessary to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

8. Health and safety

Staff and other authorised users who work in council offices will be provided with an appropriate workstation.

8.1 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment.

8.2 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the clerk.

8.3 If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the clerk or the council's IT provider.

9. Password and Authentication Policy

9.1 All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification-for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

9.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel.

9.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a council-approved, encrypted password manager.

9.4 Password Change Requirements

- Immediately change password if compromise is suspected.

9.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident

9.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices.

10 Monitoring

10.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

10.2 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc. for Monitoring and Record-keeping Purposes) Regulations 2018.

10.3 Monitoring of an employee's email and/or internet use will be conducted in

accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

10.4 The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

10.5 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

10.6 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

10.7 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

10.8 The council has software and systems in place that can monitor and record all internet usage. A daily log is kept of all activity, which details the names of all websites accessed, along with the date and time of access, by individual councillors, staff, and other authorised users. Records of internet use and sites visited will normally be retained for a period of six months.

10.9 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

10.10 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

10.11 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

11 Remote working

11.1 Increased IT security measures apply to those who work away from their

normal place of work (e.g. whilst travelling, working from home or at non-council premises as follows:

- If logging into the council's systems or services remotely, any passwords must not be saved, and the user must log out at the end of the session. The location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc.
- Any data printed should be collected and stored securely.
- All electronic files should be password protected.
- Papers, files or computer equipment must not be left unattended at a non-council premises unless arrangements have been made with a responsible person for them to be kept in a locked room or cabinet if they are to be left unattended at any time.
- Any data should be kept safely and should only be disposed of securely.
- Papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed.
- Where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

11.2 Those issued with a 'dongle' to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of internet access can be very high. Dongles should therefore be used for essential council purposes only, especially if abroad.

11.3 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

12 Website & Accessibility

12.1 Website Compliance and Publication of Documents

12.1.1 The Town Council website must meet the accessibility Web content Guidelines 2.2 AA (WCAG 2.2 AA) and The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.

12.1.2 The accessibility requirement under the regulations requires the

Council to make the website or mobile application accessible by making it perceivable, operable, understandable and robust;

12.1.3 An up-to-date Accessibility Statement must be published, and regular audits for accessibility, broken links, and compliance must occur.

12.1.4 The accessibility statement must be a comprehensive and clear statement on the compliance of the Council's website or mobile application with these Regulations.

12.2 Freedom of Information (FOI) Publication Scheme

12.2.1 All websites must include published documentation as specified in the Freedom of Information Act 2000 and the Transparency code for smaller authorities (where applicable).

12.2.2 Council documentation to be published and maintained includes Town council agendas and minutes, AGAR, councillor information, expenditure exceeding £500, procurement information, Local Authority Land, Grants, organisational chart, senior salaries, policies etc.

13 Email

13.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

13.2 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

13.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the clerk or the council's IT provider rather than assuming they know the right answer.

13.4 All councillors, staff, and other authorised users who need to use email as part of their role will be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

13.5 All council business must be conducted using council-issued email accounts hosted on an authority-owned domain.

13.6 Email messages sent on the council's account are for council use only. Personal use is not permitted.

13.7 All users must adopt a professional tone and observe appropriate email etiquette when communicating on Council business. Staff must use the Council's standard email signature and disclaimer.

13.8 Users should be aware that emails may be disclosed in legal proceedings or in response to statutory information requests. Deleted emails may remain recoverable from Council systems.

13.9 Abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails must not be sent using Council systems.

13.10 Users must not send or forward chain mail, junk mail, inappropriate jokes or gossip, unnecessarily copy recipients into correspondence, or send messages from another person's email address without authorisation.

13.11 Access to web-based personal email accounts, including Gmail and Hotmail, is not permitted on Council computer systems.

13.12 Staff must use the Council's standard Out of Office format when notifying internal and external contacts of their absence.

13.13 Users must exercise caution when receiving unsolicited or suspicious emails. They must not reply to suspicious messages, open attachments or click links where a security risk is suspected. Suspected viruses or malware must be reported immediately to the Town Clerk and Acronyms.

14 Use of the Internet

14.1 Copyright

14.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

14.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

14.1.3 Councillors, staff and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

14.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

14.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the clerk if unsure about anything.

14.2 Trademarks, links and data protection

14.2.1 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the clerk.

14.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which is available from the Council's website.

14.3 Accuracy of information

14.3.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

14.4 Use of social media

14.4.1 Councillors, staff and other authorised users must comply with the Council's applicable Social Media Policy. Council social media accounts may only be accessed or managed by authorised persons. Users must not disclose confidential Council information, impersonate others, or publish content on behalf of the Council without appropriate authorisation. Suspected misuse must be reported to the Town Clerk.

14.5 Internet Access and Restrictions

14.5.1 Internet access provided by the Council is for official Council business. Any exceptions must be authorised by the Town Clerk.

14.5.2 Users must not access websites or download material that is Illegal, offensive, discriminatory, inappropriate or likely to bring the Council into disrepute.

14.5.3 The Council reserves the right to block or restrict access to websites where necessary for security or operational reasons.

14.5.4 Employees must not use Council systems to access online radio, audio or video streaming services, instant messaging or social networking websites, except where specifically authorised for Council business.

15 Data Protection Act 2018 & UK GDPR

15.1 The Council will comply with the UK GDPR and Data Protection Act 2018. All users must process personal data lawfully, fairly and securely in accordance with the Town Council's Data Protection Policy.

16 Misuse

16.1 Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including Code of Conduct complaints against councillors or disciplinary proceedings including, in serious cases, dismissal against employees.

16.2 Prohibited use of Council IT systems includes, but is not limited to:

(a) Accessing, creating, transmitting or downloading pornographic, obscene, offensive or unlawful material;

(b) Creating or distributing discriminatory, harassing, derogatory or defamatory material;

(c) Unauthorised disclosure of confidential Council information or personal data;

(d) Installing or distributing unauthorised software;

(e) Infringing copyright or intellectual property rights; and

(f) Using Council systems in a manner that may expose the Council or individuals to criminal or civil liability.