Stone
Town Council

Information Technology Policy

April 2026

Contents

Purpose of the IT Policy

The purpose of this IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. The policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council’s data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Monitoring of IT Use

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. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council and should be read alongside the separate guidance notes on the use of Council iPads and the use of removable media.

Computer Use

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes. Reasonable personal use is, however, permitted as determined by the Town Clerk. Personal use of council computers and systems should be restricted to official lunch breaks or before or after working hours where possible, and in any case should have minimal impact on the Council's working.

1.1.2 Locking computers when leaving desk, all councillors, users should lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work.

1.1.3 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.

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

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

1.1.6 Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software) unless previously authorised by the Town Clerk.

1.1.7 Personal disks, USB sticks, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Town Clerk.

1.1.8 The council has a number of wireless networks. Using any device, such as a mobile phone, to make a personal Wi-Fi hot spot which bypasses existing Wi-Fi is not pereemitted.

Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

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

2.1.3 All portable computers must be stored safely and securely when not in the office, i.e. when travelling or when working from home. Portable equipment should not be left unattended when away from council premises or home, and should never be left in parked vehicles unless securely locked out of sight in the boot.

2.1.4 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.

2.1.5 Multi-Factor Authentication (MFA) should be implemented wherever possible.

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the Town Clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to make a contribution to replacement costs, where not covered by insurance.

2.1.7 No photographs or videos may be taken on council premises that may risk revealing confidential information, unless it has been authorised by the Town Clerk, This includes the use of mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.8 Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present, other than to the extent required for minute taking only. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.1.9 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 Town Clerk.

2.2 Use of own devices

2.2.1 Personal laptops and other computers or other devices should not be used to access council IT systems, unless this is in accordance with the exceptions below, or has been specifically authorised by the Town Clerk. This is to ensure that no viruses enter the system, to assist in maintaining security, confidentiality, and data protection.

2.2.2 The exceptions to the above are:

- Access to the council's remote AVD system by authorised users.
- Access to the Council's telephone system by authorised users.
- The use of personal devices by authorised users to access council email accounts and related calendar etc. information.
- Connection to the Council's Wi-Fi, without any access to Council data that would not otherwise be accessible to the user.

2.2.3 Where council data is stored on a personal device as a result of any of the above, it should be stored securely and protected by passwords and PINs. No council data should be solely stored on a personal device, and must also be stored on an official council device to allow for data backup.

2.2.4 The Town Clerk should be informed should any personal device on which Council data is stored be lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent lost/stolen phones being used, users will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.5 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.

2.2.6 In cases of legal proceedings, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve relevant data.

2.2.7 Prior to the disposal of any device that may have council data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to delete any data relating to the Council. The council may, at its discretion, seek proof that this has been done.

2.2.8 Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and safety

3.1.1 Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

3.1.2 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. Further details are set out in the council's health and safety policy.

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must raise this with the Town Clerk.

3.1.4 If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Town Clerk, or raised direct with the Council IT support provider.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords[1]. 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.

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

4.1.2 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 by the council's IT support with the permission of the Town Clerk and appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel, with a copy in a sealed envelope stored in the council's safe, only to be accessed in an emergency.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords may be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass).

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- A log should be kept of all systems, and which users have access to administrative credentials for those systems. Any access to the emergency copy of those credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident.

4.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.
- System administrators, including the Council's IT Support contractor, may set up initial passwords, which users should be advised to change.

[1] The council is considering adopting 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.

Monitoring

5.1.1 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.

5.1.5 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.

5.1.6 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.

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors and IT support provider 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.

5.1.8 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.

5.1.9 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.

5.1.10 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.

5.1.11 The council may implement software and systems that can monitor and record all internet usage.

5.1.12 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.

5.1.13 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.

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

Remote working

6.1.1 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 any other different venue), as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved locally. Access to the Council's systems remotely via a web browser is not permitted.
- 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
- papers, files or computer equipment must not be left unattended at non-council premises (excluding home working) unless arrangements have been made with a responsible person at those premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time.
- council equipment and data should be stored securely when working from home.
- 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 out of sight 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;

Email

7.1.1 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.

7.1.2 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.

7.1.3 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 Town Clerk, rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally 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.

7.1.5 Email messages sent on the council's account are for council use only. Personal use is not permitted, other than in an emergency.

Use of the Internet

8.1 Copyright

8.1.1 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.

8.1.2 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.

8.1.3 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).

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

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

8.2 Trademarks, links and data protection

8.2.1 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 Town Clerk.

8.2.2 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 provided in the electronic Councillor’s Handbook, and can be requested from the Town Clerk at any time.

8.3 Accuracy of information

8.3.1 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.

Use of social media

9.1.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

9.1.2 Personal use of social networking/media and chat sites during working hours should be restricted to breaks.

9.1.3 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual’s position, this is acceptable, but should always comply with the council’s Press and Media Protocol.

9.1.4 Inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal weblogs and social media postings, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

9.1.5 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

9.1.6 It is important to note that external contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data including contact details from any personal device/equipment.

Misuse

9.1.7 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 disciplinary proceedings or, in serious cases, dismissal.