Introduction

The purpose of an 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. A well-defined 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.

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.

Computer use

Hardware

1.1.1 All staff will be provided with a laptop computer. Council computer equipment is provided for council purposes only.

1.1.2 Staff who work from home or who are required to work out of the office will be provided with a mobile phone.

1.1.3 All councillors, staff, and other authorised users must lock their computers 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.

1.1.4 All computer and other electronic equipment supplied by the Council 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.

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

1.1.6 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.

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

1.1.8 Councillors, staff, and other authorised are not to purchase or use any computer or mobile equipment (including software) for Council business unless previously authorised by the Proper Officer. Any personal equipment used to store Council data must be registered with the Proper Officer.

1.1.9 USB sticks and other data storage devices may be used on council computers for

backup purposes or for data access when online connectivity is not available. Any such equipment must be purchased by the Council and will be recorded in the Council's asset register.

1.1.10 Any faults or necessary repairs to council equipment must be reported to the Proper Officer.
Faults or repairs to personal equipment is the responsibility of the owner.

1.2 Portable equipment

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

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

1.1.13 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. 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 visible in parked vehicles.

1.1.14 It is important to ensure all portable devices used by staff are protected with PIN codes or face ID in case they are lost or stolen. All smartphones or tablets, including personal devices, that hold council data, e.g. emails and files, must be protected with a pin code. Any security set on these devices must not be disenabled or removed.

1.1.15 If an item of portable equipment is lost or damaged this should be reported to the Proper Officer. This includes loss of any personal equipment that may contain council data. If the loss or damage of council equipment is due to an act of negligence, the individual responsible may be liable to meet the first £100 of the loss/damage to laptops and £50 for mobile phones.

1.1.16 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 on council premises, without the prior written permission of the Proper Officer. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

1.1.17 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).

1.1.18 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 Proper Officer.

2 Use of own devices

2.1 Personal laptops should not be brought into work and used to access council IT systems by employees during working hours, unless this has been authorised by the employee's line manager. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.

2.2 The Council recognises that some councillors, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's online system or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.3 The same security precautions apply to personal devices as to the council's laptop equipment. For continuity purposes, calls made by employees to external parties must be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers.

2.4 Any emails sent from personal as opposed to Council owned devices must be sent from a council email account and must not identify the individual's personal email address. Auto-forwarding of emails to personal email addresses will not be permitted. Emails are not to be manually forwarded to Councillor's personal email addresses.

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.

2.6 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.

2.7 Use of personal devices is discouraged. However, when using personal devices the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using

different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.8 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a 6-digit pin or strong password to protect their device(s) from being accessed.;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than10 minutes;
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately, preferably by a means other than email (this is particularly relevant to documents sent to the Staffing Committee);
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the Proper Officer if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they 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.

2.9 Personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.10 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

2.11 Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

2.12 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users may be required to allow the Council's IT support provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.13 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.

3. Health and safety

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

3.2 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.

3.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Proper Officer.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Proper Officer.

4. Password and Authentication Policy

4.1 All user accounts should 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:

- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- 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.

4.2 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 to be accessed only in an emergency.

4.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.

4.4 Password Change Requirements

- Passwords should be routinely changed every 60 days
- Passwords should be Immediately changed password if compromise is suspected.

4.5 Password Access Control and Logging

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

4.6 Responsibility

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

5. Remote working

5.1 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 venue, as follows:

- council services should not be accessed from any device that is not owned by the Council or the user;
- 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 sensitive electronic files should be password protected and the data saved to the council's system/services when accessible;
- 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;

5.2 Use of publically accessible Wi-Fi, for example at airports is not permitted unless approved by the Proper Officer.

6. Email

6.1 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.

6.2 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.

6.3 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 Proper Officer rather than assuming they know the right answer.

6.4 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.

6.5 Email access will automatically be removed when councillors, staff or other authorised users leave the Council.

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

7. Use of the Internet

7.1 Copyright

7.1.1 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.

7.1.2 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.

7.1.3 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).

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

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

7.2 Trademarks, links and data protection

7.2.1 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 Proper Officer.

7.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy.

7.3 Accuracy of information

7.3.1 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.

8. Use of social media

8.1 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.

8.2 Personal use of social networking/media and chat sites are not permitted during working hours.

8.3 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.

However, 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 residents or other local organisations may read councillors, staff, and other authorised users' personal weblogs, 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.

8.4 To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not

represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.

- Employees may not develop a site or write a blog that will mention the council, with the exception of the Council's Communications Officer.
- The council expects councillors, staff, and other authorised users to be respectful about the council and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos or videos that include employees should not be posted on social media without explicit permission
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations should not take place on any social networking sites, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors, staff, and other authorised persons must only be done by the Council's Communications Officer. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.
- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website) in a personal capacity. Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.
- Contacts by the media relating to the council, should be referred to the Council's Communications Officer.
- Staff who use social media sites on behalf of the Council (currently restricted to the Communications Officer) must ensure that the information on their profile is accurate and up to date. They must ensure they provide the council with login details,

including password(s), so that these sites can be accessed and updated in their absence.

- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other authorised users on any social media/networking sites.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff, or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

8.5 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.

8.6 It is important to note that 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.

9. Misuse

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

Date of Policy	Approving Committee	Date of Committee Meeting	Policy Reference Version	Supersedes	Adopted by Council	Date for next review
April 2026	Council	18/05/2026	1	N/A	18/05/2026	March 2027