INFORMATION TECHNOLOGY (IT) POLICY

PURPOSE OF THE IT POLICY	**2**
MONITORING OF IT USE	**2**
SCOPE OF THIS POLICY	**2**
COMPUTER USE	**2**
EQUIPMENT	**3**
HEALTH AND SAFETY	**6**
PASSWORD AND AUTHENTICATION POLICY	**6**
MONITORING	**7**
REMOTE WORKING	**9**
EMAIL	**9**
USE OF THE INTERNET	**10**
USE OF SOCIAL MEDIA	**11**
MISUSE	**14**

This IT Policy was adopted by the Council at its meeting held on XX YYYY 2026

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. 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.

Councils will also need to determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

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.

Computer use

1.1 Hardware

1.1.1 Council computer equipment is provided for Council purposes; however reasonable personal use is permitted (reasonable interpreted as in the opinion of the Clerk). Any personal use of our computers and systems should not interrupt daily Council work. Staff and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

1.1.2 Locking computers when leaving desk, 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.

DRAFT

1.1.3 All computer and other electronic equipment supplied should be treated with good care. 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 All Council computer equipment is logged against the current owner of that equipment. A database of equipment issued will be kept.

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

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

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

1.1.9 The Council has a number of wireless networks. Using a portable device to make personal Wi-Fi hot spots which bypass existing WiFi is not allowed.

1.1.10 Any faults or necessary repairs must be reported to the Clerk / the Council's external IT support.

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 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. Equipment should not be left unattended when away from Council premises and should not be left in cars, except where it is entirely unavoidable for short periods, in which case equipment must be locked in the boot of the car.

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. Any security set on these devices must not be disenabled or removed.

DRAFT

2.1.5 Multi-Factor Authentication (MFA) is not enabled. 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).

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the Clerk / the Council's external IT support.

2.1.7 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 Clerk. This includes 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. 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 Clerk / the Council's external IT support.

2.2 Use of own devices

2.2.1 Personal laptops and other computers or other devices should not be brought into work and used to access Council IT systems, unless this has been authorised by the Clerk. 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.

2.2.2 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.

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

2.2.4 Wherever possible 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

DRAFT

work and personal profiles, the work profile must always be used for work-related purposes.

2.2.5 Councillors and other authorised users who intend to use their own devices via the Council's infrastructure must ensure that they:

- use a strong password to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 3 failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 1 hour.
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from Council data where possible;
- 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 Clerk / the Council's external IT support 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.

2.2.6 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 (e.g. google drive) 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.

2.2.7 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.

2.2.8 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

2.2.9 Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted after use. The Clerk / the Council's external IT support will provide assistance or training in doing this if needed. Additional risks include data belonging to the Council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

2.2.10 Any work done on user's own equipment should be stored securely and password protected and should be backed up.

2.2.11 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

2.2.12 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 are required to allow the Council's external IT support access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.13 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 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 computer user who feels that their workstation requires changes to make it compliant must speak to the Clerk.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk / the Council's external IT support.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The Council's external IT provider 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.

Multi-Factor Authentication (MFA) is enabled for online banking. 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.

DRAFT

Additional 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.

The Council recommends these practices as part of its commitment to information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

4.1.2 Access to Passwords

- Passwords are personal and must not be shared, unless in exceptional cases, approved by the Clerk in conjunction with the Chairman of the Council.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response, employee absence beyond holidays and short-term absence, employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- In exceptional cases (e.g., incident response, employee absence beyond holidays and short-term absence, employee offboarding), online banking passwords and multi-factor authentication co-ordination and sharing of passcodes require the approval of Council.

4.1.3 Password Storage and Management

- Passwords must only be stored in secure locations.
- Copies of staff logon and passwords to online banking is physically held in a secure location addressed to the Chairman of the Council.
- Passwords can be stored using Microsoft Edge logged in only via a Council domain. The exception is bank login details, especially if multi-factor authentication process is not enabled.
- Passwords can be stored in an approved, encrypted password manager vault.

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 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.

4.1.6 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.

Monitoring

DRAFT

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 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.

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 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.

5.1.12 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.

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

DRAFT

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 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, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the devise does not clearly support these actions (for example at an internet café), Council services should not be accessed from that device;
- the location and direction of the device or 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 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 at the non-Council premises for the items 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.

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

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although the use of email is a vital means of communication, 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.

DRAFT

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 Council's external IT support 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.

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 Clerk / the Council's external IT support if unsure about anything.

DRAFT

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 Clerk / the Council's external IT support.

8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, refer to the Employee Handbook. Further information on the Council's data protection policies can be found on the website.

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 should be restricted to breaks during working hours, or after hours with permission.

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.

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 about the Council 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, 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.

DRAFT

9.1.4 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.
- Any employee who is developing a site or writing a blog that will mention the Council, e.g. our current or potential plans, Councillors, staff, and other authorised users, partners, must inform the Clerk that they are writing this and gain agreement before going 'live'.
- The Council expects Councillors, staff, and other authorised users to be respectful about the Council and its current or potential staff, including employees, Councillors, Clerk, and authorised users 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 or other workers wearing uniforms or clothing displaying the Council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the Council. Additionally, photos, videos, or audio recordings must not be taken on Council premises 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 with external stakeholders e.g. residents 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, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. 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

DRAFT

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). 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.
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the Council or its Councillors, staff, and other authorised users, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the Council, should be referred to the Clerk.
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the Council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for Council development purposes 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 LinkedIn, Facebook, X.com or any other 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.

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 the Council 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

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.

DRAFT