Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
email: info@fakenhamtownCouncil.gov.uk
website: fakenhamtownCouncil.gov.uk

Fakenham Town Council

IT POLICY

Contents:

1. Introduction

Fakenham Town Council ("the Council") recognises the importance of effective, secure, and lawful use of information technology (IT) and email systems in supporting its governance, operations, and communications.

This policy sets out the standards and responsibilities for the appropriate use of Council IT systems and related technology by Councillors, employees, volunteers, contractors, and other authorised users. It supports compliance with the Smaller Authorities Proper Practices Panel - Practitioners' Guide 2025, relevant UK data protection legislation, and good practice standards.

This policy forms part of the Council's Digital Governance Framework and must be read in conjunction with the following related policies:

- Councillor Email Policy
- Information Transfer Policy
- Removable Media Policy
- Social Media and Communications Policy
- Data Protection Policy
- Records Management and Retention Policy
- Members' Code of Conduct

The IT Policy provides the overarching framework for digital security, acceptable use, monitoring, and incident management. Supporting policies provide operational or role-specific guidance and must not contradict the IT Policy.

Where overlap exists between policies, the requirements of the IT Policy shall take precedence.

Failure to comply with any of the above policies may result in formal action in accordance with the Council's disciplinary procedures and, where applicable, statutory obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Freedom of Information Act 2000.

2. Scope

This policy applies to all Councillors, staff, and other authorised users, regardless of working location or pattern, including home-based, office-based, flexible, or part-time arrangements. It covers:

- IT equipment and systems provided by the Council; and
- Personal devices and systems used to access, process, or store Council information.

The policy establishes expectations for the secure, lawful, and appropriate use of Council systems and data and sets out responsibilities for all users.

Councillors, employees, contractors, and other authorised users should be aware that the Council may monitor the use of its IT systems where there is a legitimate and lawful reason for doing so. By using Council systems, users acknowledge that proportionate monitoring may take place. Responsibility for authorising and overseeing monitoring activity rests with the Clerk. Detailed information about monitoring, including scope, purposes, retention, data sharing, and data protection rights, is provided in Section 7 (Monitoring) of this policy. Monitoring will always be conducted proportionately, in accordance with UK data protection legislation, and will be restricted to Council systems and data.

3. Computer Use – Hardware

3.1 Council computer equipment is provided primarily for official Council business. Limited and reasonable personal use is permitted, provided that such use does not interfere with Council duties, incur additional cost, compromise security, or breach this policy. Users must adhere to ethical standards, respect copyright and intellectual property rights, and must not access inappropriate, unlawful, or offensive content.

3.2 Councillors, staff, and other authorised users must lock computers or devices when left unattended to prevent unauthorised access. This applies to both Council-issued devices and personal devices used for Council work. Failure to comply may result in appropriate action in accordance with the Council's governance or disciplinary procedures.

3.3 All computer and electronic equipment supplied by the Council must be used and handled with due care. Such equipment represents a significant investment by the Council, and damage or loss may result in financial cost.

3.4 Users must take reasonable steps to protect equipment from avoidable risks, including damage caused by food, drink, contamination, or improper storage.

3.5 All assigned computer and mobile equipment will be recorded and issued to a named recipient, who will acknowledge receipt. A central record of issued equipment will be maintained and cross-referenced with the Council's Asset Register.

3.6 Council-issued equipment must not be dismantled, modified, or reassembled without prior authorisation.

3.7 Councillors, staff, and authorised users must not purchase computer or mobile equipment (including software) for Council use without prior authorisation.

3.8 Unauthorised installation of software on Council-issued devices is prohibited due to security risks.

3.9 Personal removable storage devices (including USB sticks, external drives, CDs or DVDs) must not be used on Council-issued computers without prior approval from the Clerk.

3.10 When using Council premises or Council networks, users must not create or access alternative Wi-Fi connections or portable hotspots that bypass the Council's authorised wireless networks, as this may introduce security vulnerabilities.

3.11 Routine IT issues, maintenance requirements, or technical support requests should be reported to the Council's appointed IT provider, ICO Systems Ltd. Any hardware faults or equipment requiring repair or replacement must also be reported to the Clerk.

4. Equipment

4.1 Portable Equipment

4.1.1 Portable equipment includes laptop computers, tablets, mobile and smart phones with email capability, and any other device capable of accessing Council systems or storing Council information.

4.1.2 Council backup and data protection procedures applicable to portable equipment must be followed at all times, in accordance with the Council's approved backup and information security arrangements.

4.1.3 All portable IT equipment must be used, handled, and stored in a manner that protects both the device and any information stored on it, whether on Council premises, offsite, or at home. Users must ensure that portable equipment:

- Is not left unattended in public or unsecured locations;
- Is kept within sight or close possession when used outside a secure environment;
- Is secured in a locked office, cabinet, or other approved secure location when not in use;
- Is not left in vehicles unless no reasonable alternative exists and the device is concealed and secured;
- Is handled with due care to prevent loss, damage, or unauthorised access.

4.1.4 All portable devices used to access or store Council data must be protected by encryption where supported and secured by a PIN, password, or biometric authentication. Where technically available, devices should be configured to restrict or erase data after repeated unsuccessful access attempts. Security settings must not be disabled.

4.1.5 Users are responsible for maintaining the security of their accounts and passwords. Passwords must be strong, unique, and must not be shared with others. Multi-Factor Authentication (MFA) must

be enabled wherever available and is mandatory for all accounts with access to sensitive Council data, including but not limited to Council email, financial systems, HR records, and other restricted systems. MFA significantly reduces the risk of unauthorised access and supports compliance with the UK GDPR and the Data Protection Act 2018.

4.1.6 Loss, theft, or damage to portable equipment must be reported immediately to the Clerk. Where loss or damage results from proven negligence, the Council reserves the right to seek appropriate reimbursement in accordance with contractual, employment, or governance arrangements.

4.1.7 Photographs, video, or audio recordings must not be taken on Council premises where this would compromise confidentiality, data protection obligations, or the privacy of individuals. Recording of non-public meetings or confidential discussions is prohibited without the consent of those present. This does not affect statutory rights under the Openness of Local Government Regulations 2014 in relation to public meetings.

4.1.8 Webcams and recording functionality on portable devices must only be used for legitimate Council business purposes.

4.2 Use of own devices

4.2.1 The Council recognises that Councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops, or other devices to access Council email accounts, servers, approved cloud platforms, or networks for legitimate Council purposes. Any such use of personal devices is subject to compliance with this policy. Personal devices must be kept up to date, with operating systems and software patched and updated promptly to address known vulnerabilities. Council data must not be stored on personal devices except via Council-approved systems (for example, Council email accounts or approved cloud platforms).

4.2.2 The same standards of security, confidentiality, and acceptable use apply to personal devices as to Council-issued equipment when used for Council business.
For continuity and data protection purposes:

- Calls to external stakeholders should be made using Council landlines or Council-issued mobile numbers wherever practicable;
- Emails must be sent from a Council email account and must not identify or rely upon a personal email address for Council business.

4.2.3 Councillors, staff, workers, contractors, and other authorised users accessing Council systems must use all devices in an ethical and lawful manner. Accessing inappropriate, unlawful, or offensive material via Council systems or infrastructure is prohibited, irrespective of device ownership.
For employees, breaches may result in disciplinary action, including summary dismissal where appropriate. For workers or contractors, this may result in termination of the relevant agreement.

4.2.4 In the event of legal proceedings, investigation, subject access request, or other lawful requirement, the Council may require access to relevant Council data held on a personal device. Users must cooperate in providing access to Council-related information where lawfully required. The Council will not seek access to personal data unrelated to Council business.

4.2.5 Users must maintain a clear separation between Council data and personal data wherever possible. This may include:

- Using separate applications for Council email;
- Using a dedicated work profile where supported by the device;
- Avoiding the mixing of Council documents with personal files.

4.2.6 Councillors, staff, and other authorised users using personal devices for Council business must ensure that:

- The device is protected by a strong password, passphrase, PIN (minimum 6 digits), or biometric authentication. Users should combine these methods where supported for optimal security.
- Automatic screen lock is enabled after a short period of inactivity (recommended maximum 5 minutes).
- The device is configured to restrict access or automatically erase data after repeated failed login attempts, where supported.
- Up-to-date antivirus software (where applicable) and system updates are installed and maintained.
- Only secure Wi-Fi networks are used. Public or unsecured wireless networks must not be used to access sensitive Council information unless a secure connection (e.g., VPN or encrypted protocol) is in place.
- Work-related data cannot be accessed by family members or other third parties who may use the device.
- The Clerk is informed immediately if the device is lost, stolen, or accessed inappropriately where there is any risk to Council data.

4.2.7 Council data must not be permanently stored on personal devices. Documents downloaded for working purposes must be deleted once no longer required. The official Council system remains the primary and authoritative storage location for all Council records.

Council data must not be backed up, synchronised, or saved to personal cloud storage accounts (for example personal Google Drive, Dropbox, personal Microsoft OneDrive, iCloud or similar services).

Special category data and particularly sensitive information (including safeguarding matters, personnel records, disciplinary information, DBS information, or financial account details) must not be downloaded, stored, or processed on personal devices.

Where a Councillor ceases to hold office, or a member of staff leaves employment, all Council data held on personal devices must be permanently deleted without delay.

4.2.8 If removable media are used to transfer Council data (e.g. USB drives or CDs), data must be securely deleted from the media once the transfer is complete.

4.2.9 When transferring Council data electronically, this must be done using secure and encrypted channels (for example via secure email, VPN, or HTTPS connections). Unsecured wireless networks must not be used for transferring sensitive information.

4.2.10 Prior to disposal of any personal device used for Council business, and upon a Councillor or staff member leaving the Council, users must ensure that all Council-related accounts, access credentials, and identifiable Council data are removed from the device. The Clerk or the Council's appointed IT provider must verify that all Council data has been permanently deleted and that all Council accounts and access credentials have been deactivated. Guidance and support may be provided by the IT provider where required.

4.2.11 Users are responsible for the maintenance, insurance, and repair of their personal devices. The Council accepts no liability for loss of personal data, hardware failure, or damage to personal devices

used for Council business. The Council will use reasonable endeavours to provide guidance in relation to Council systems but cannot guarantee compatibility or technical support for personal equipment.

5. Health and Safety

5.1 Councillors, staff, and other authorised users who work in Council offices will be provided with an appropriate workstation, including furniture and equipment suitable for safe and comfortable use.

5.2 The Council has a duty to ensure that regular eye tests, carried out by a competent person, are offered to employees using display screen equipment (VDUs), in accordance with the Health and Safety (Display Screen Equipment) Regulations 1992.

5.3 Any VDU user who believes their workstation requires adjustment to meet ergonomic or safety requirements should contact the Clerk.
If any hazards are identified at a workstation, including unusual noises or malfunctions from IT equipment, these must be reported immediately to the Clerk.

6. Password and Authentication Security

6.1 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 provides strong protection against common cyber threats such as brute-force attacks while remaining memorable. 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 a mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data.

To further strengthen account security:

- Initial user account passwords must be generated by the Council's IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- These practices support robust information security and 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.

6.2 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 specific cases (e.g., incident response, Councillor or staff offboarding, or device seizure as per Section 5.2.4), access to system credentials may be granted to authorised personnel, including IT provider staff, with prior approval and logging overseen by the Clerk.
- Administrative credentials (e.g., system or service administrator accounts) must be stored securely in a Council safe. Access is limited to authorised personnel and the Clerk. A written log of any access must be maintained. Where feasible, a secondary secure electronic backup using a Council-approved encrypted password manager may also be maintained to support emergency recovery, with access restricted and auditable.

6.3 Password Storage and Management

- Passwords must never be stored in plain text or written down in unsecured or publicly accessible locations.
- Administrative credentials may be stored as a hardcopy in a secure Council safe, accessible only by authorised personnel and the Clerk. A written log of any access must be maintained.
- Where appropriate, a secondary electronic backup may be stored in a Council-approved encrypted password manager (e.g., LastPass, Bitwarden, KeePass), with access restricted, auditable, and overseen by the Clerk.
- All other user passwords (non-administrative) should be managed using best practice standards, including password managers where possible, in line with NCSC guidance.
- Users must ensure any personal storage of passwords for Council systems (e.g., on personal devices) is avoided, except through Council-approved encrypted password managers.

6.4 Password Change Requirements

- Passwords must be changed immediately if compromise is suspected.
- Routine password changes are recommended in line with IT provider guidance and best practices.

6.5 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 in accordance with Council IT incident procedures.

6.6 Responsibilities

Users are responsible for:

- Creating and maintaining secure passwords for their accounts.
- Protecting credentials in accordance with this policy and reporting any suspected compromise immediately.

The Clerk (or designated Council officer) is responsible for:

- Enforcing this password policy across all Councillors, staff, and authorised users.
- Monitoring compliance and taking appropriate action if policy requirements are not met.
- Liaising with the IT provider to ensure technical controls (e.g., MFA, password managers, system settings) are in place.
- Maintaining records of password policy enforcement, incidents, and approvals for exceptional access.

The Council's IT security provider is responsible for:

- Managing system/service credentials and ensuring secure password creation.
- Implementing technical controls to support the password policy, such as MFA, encryption, and audit logging.
- Assisting the Clerk with auditing and reporting where technical systems allow.

7. Monitoring

7.1 The Council reserves the right to monitor and maintain logs of computer usage and inspect files stored on its network, servers, computers, or associated technology where necessary to ensure compliance with this policy and relevant legislation. Internet, email, and computer usage may be monitored where necessary for security purposes, system maintenance, fault investigation, or the prevention and detection of unauthorised or unlawful activity.

7.2 The Council will monitor the use of electronic communications and internet access in accordance with UK data protection legislation, including the UK GDPR and the Data Protection Act 2018, and in line with relevant Information Commissioner's Office (ICO) guidance on workplace monitoring.

7.3 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment carried out by the Council to ensure that monitoring is necessary, proportionate, and justified. Monitoring is undertaken in the Council's legitimate interests, including ensuring compliance with this policy, protecting Council systems, and safeguarding Council data.

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

7.5 The information gathered through monitoring will be retained only for as long as necessary for security, system management, or investigation purposes, and in accordance with the Council's data retention policy.

7.6 Councillors, staff, and other authorised users have rights in relation to their personal data, including the right to make a subject access request and, in certain circumstances, to request rectification or erasure of data. Further details of these rights and how to exercise them are set out in the Council's Data Protection Policy.

7.7 Such monitoring and, where necessary, retrieval of the content of messages may take place for legitimate purposes, including verifying appropriate use of Council systems, recovering lost or corrupted data, investigating suspected misconduct or security incidents, or complying with a legal obligation.

7.8 Where technically available, Council systems may generate audit logs recording internet activity, including websites accessed, dates and times of access, and associated user accounts. Such logs will be retained for a defined period in accordance with the Council's retention schedule (for example, six months), after which they will be securely deleted unless required for an ongoing investigation.

7.9 The Council reserves the right to inspect files stored on its computer systems where necessary to ensure compliance with this policy. The Council may also monitor use of Council systems at any time they are accessed, in order to prevent misuse, protect the Council's reputation, and safeguard systems from security threats. Monitoring will be restricted to Council systems and data and will not extend to purely personal information unrelated to Council business.

7.10 Any use of Council systems that is considered improper, excessive, unlawful, or in breach of this policy may result in disciplinary proceedings, or termination of engagement in the case of contractors or other authorised users.

7.11 All Council computers and systems will be periodically checked and scanned for unauthorised programmes, malware, and viruses as part of routine security maintenance.

8. Remote working

8.1 Increased IT security measures apply to Councillors, staff, and other authorised users who work away from their normal place of work (for example, whilst travelling, working from home, or working from an external venue), as follows:

- If logging into the Council's systems or services remotely using a device that does not belong to the Council, users must not save passwords or login credentials on that device and must log out fully at the end of the session. Council systems must not be accessed from shared or public computers (for example, internet cafés or publicly accessible terminals) where secure configuration cannot be assured;
- Access to Council systems must comply with the security requirements set out in Sections 4 and 6 of this policy, including the use of strong passwords and Multi-Factor Authentication (MFA) where enabled;

- The location and positioning of screens must be checked to ensure that confidential information cannot be overlooked. Appropriate steps must be taken to prevent unauthorised viewing, including when working on public transport or in public places;

- Any printed material containing Council information must be collected immediately from printers and stored securely. Printing should be avoided unless strictly necessary;

- Electronic files containing Council data must remain within Council-approved systems and platforms. Files must not be downloaded to unsecured local storage. Where files are temporarily downloaded for working purposes, they must be deleted once no longer required;

- Papers, files, removable media, or computer equipment must not be left unattended at non-Council premises unless stored in a locked room, cabinet, or other secure location;

- Council data (including papers, files, USB drives, or backup devices) must not be left unattended in vehicles except where unavoidable and only for short periods. In such cases, items must be concealed and locked in the boot. When staying away overnight, Council data and devices must be taken into secure accommodation and protected from unauthorised access or damage;

- Where technically supported, mobile devices used to process sensitive Council information must have remote location tracking and remote wipe capability enabled;

- Councillors, staff, and authorised users handling sensitive data away from Council premises should use a screen privacy filter where appropriate and ensure devices are locked when not in use.

8.2 Where Council-issued mobile connectivity devices (such as mobile data devices or similar technology) are provided to enable remote internet access, these must be used for essential Council purposes only. Users must be mindful of potential data roaming charges, particularly when travelling abroad, and must seek prior approval where significant costs may be incurred.

8.3 Where paid Wi-Fi access is required (for example, at transport hubs or hotels), usage must be limited to essential Council business. Public Wi-Fi networks must not be used to access sensitive Council

information unless a secure, encrypted connection (such as VPN or HTTPS) is in place, in accordance with Sections 4 and 6 of this policy.

9. Email

9.1 Council email facilities are provided to support effective, secure, and timely communication on Council business. Councillors, staff, and other authorised users must use email responsibly and strictly for Council purposes. As email presents security and legal risks, users must remain vigilant against phishing attempts, malware, and other cyber threats, and must comply with the security requirements set out elsewhere in this policy.

9.2 Email should be used appropriately and proportionately. In some circumstances, matters may be resolved more effectively by telephone or face-to-face discussion rather than through extended email correspondence. Councillors, staff, and other authorised users are expected to exercise professional judgement in selecting the most appropriate communication method.

9.3 These rules are designed to minimise legal, reputational, and security risks associated with email use. If a matter arises which is not clearly covered by this policy, Councillors, staff, and other authorised users should seek guidance from the Clerk before proceeding.

9.4 Councillors, staff, and other authorised users who require email access for their role will normally be provided with an individual Council email account. The Council reserves the right to withdraw or restrict access where it is no longer required for the role, or where misuse of the system is identified, in accordance with this policy and any applicable procedures.

9.5 Email accounts provided by the Council are for Council business only. Personal use of Council email accounts is not permitted.

9.6 Councillors must use their official Council-issued email address for all Council business. Council business must not be conducted using personal email accounts. Council emails must not be automatically or manually forwarded to personal email addresses.

9.7 Council staff must not send Council business communications to a Councillor's personal email address. Where a Councillor contacts the Council using a personal email account in relation to Council business, staff should reply to the Councillor's official Council email address and remind them of the requirement to use that account for Council communications.

9.8 Users must be aware that emails created, sent, or received in the course of Council business may constitute official records. Such emails may be subject to disclosure under the Freedom of Information Act 2000, the UK General Data Protection Regulation, the Data Protection Act 2018, or other applicable legislation. Emails should therefore be drafted professionally and with the understanding that they may be disclosed to third parties in accordance with the law. Email use is also subject to the monitoring provisions set out in Section 7 of this policy.

10. Use of the Internet

10.1 Copyright

10.1.1 Much of the material available on the internet is protected by copyright and other intellectual property rights. Unauthorised copying, reproduction, distribution, or adaptation of such material, including electronic copying, may constitute an infringement of copyright and is prohibited. The

Council will comply with the provisions of the Copyright, Designs and Patents Act 1988 and related legislation.

10.1.2 Copyright protection applies not only to written documents but also to software, images, graphics, databases, audio and video content. Unlawful use of copyrighted material may expose the Council to legal liability and financial penalties and may result in disciplinary action, including dismissal in the case of employees, or termination of engagement in the case of contractors or other authorised users.

10.1.3 The ease of copying material electronically does not remove the requirement to comply with copyright law. Councillors, staff, and other authorised users must not assume that material available online may be freely copied or reused.

10.1.4 Users should be aware that information described as being in the "public domain" does not necessarily mean it is free from copyright protection. In general, copyright in literary, dramatic, musical, and artistic works expires 70 years after the death of the author, subject to statutory exceptions. Where uncertainty exists, users must seek guidance before reproducing material.

10.1.5 Website terms and copyright notices must be reviewed before downloading, copying, or reusing online content. Where permission is required, it must be obtained before use. If unsure, councillors, staff, and other authorised users should consult the Clerk.

10.2 Domain Names, Trademarks, Links and Data Protection

10.2.1 No councillor, member of staff, or other authorised user may register domain names, social media accounts, or trademarks incorporating the Council's name, branding, or insignia without prior authorisation from the Council.

10.2.2 Links from the Council's official website or digital platforms to external websites must not be created without prior approval from the Clerk. External links may create reputational, legal, or security risks and must therefore be appropriately assessed before publication.

10.2.3 The processing of personal data via online systems or platforms must comply with the Council's Data Protection Policy and applicable legislation, including the UK General Data Protection Regulation and the Data Protection Act 2018. Special category data must be handled in accordance with enhanced security and confidentiality requirements.

10.3 Accuracy and Reliability of Online Information

10.3.1 The internet provides access to a wide range of information sources. However, not all online content is accurate, reliable, or up to date. Councillors, staff, and other authorised users must exercise professional judgement when relying on information obtained from the internet for Council purposes.

10.3.2 Where online information is used to inform Council decisions, reports, publications, or public statements, reasonable steps should be taken to verify its accuracy and reliability using reputable sources.

11. Social Media, Messaging, and AI Tools

11.1 Scope and definitions

11.1.1 Social media includes blogs; user-generated content sites (e.g., YouTube); social networking sites (Facebook, LinkedIn, X, Instagram, TikTok, etc.); virtual worlds (Second Life); instant messaging apps (WhatsApp, Teams, Signal); text messaging; and more traditional media (TV, newspapers). Care should be taken when using social media or messaging tools at any time, whether using council systems or personal devices.

11.1.2 Personal use of social media during working hours is not permitted for staff. Councillors and staff should use social media responsibly outside of working hours or in their own time, ensuring personal activity does not interfere with council business, compromise council systems, or breach this policy.

11.1.3 Councillors, staff, and other authorised users may use social media, messaging apps, or AI tools in the course of their official duties to support council communications, engagement, or administration. Such use must comply with this policy, relevant data protection legislation (GDPR/Data Protection Act 2018), and copyright laws.

11.1.4 Any use of AI tools (e.g., ChatGPT, Bard, Bing AI) for council business must:

- Only involve council-approved data (no sensitive personal data unless appropriately anonymised).
- Be reviewed for accuracy before use in communications or decision-making.
- Be consistent with professional, lawful, and ethical standards.

11.2 Responsible use

11.2.1 Councillors, staff, and other authorised users must not post or share material that could:

- Compromise confidentiality or personal data.
- Defame or misrepresent the council, colleagues, or partners.
- Breach copyright or intellectual property rights.
- Constitute bullying, harassment, discrimination, or create a hostile environment.

11.2.2 Staff and councillors may use messaging apps (WhatsApp, Teams, Signal, etc.) to communicate council business without seeking prior approval, provided they follow the principles in this policy (confidentiality, security, professional conduct). Messages must be retained or archived in council-approved systems where they relate to council business.

11.2.3 Councillors, staff, and other authorised users must ensure that official council communications:

- Use council-provided accounts where available.
- Are not forwarded to personal email accounts or devices, unless specifically approved for secure storage or access in line with Sections 4.2, 8, and 9.
- Include disclaimers when expressing personal opinions online (e.g., “The views expressed here are my own and do not represent the council”).

11.2.4 Any blog, social media, or AI-generated content that references the council, councillors, staff, partners, or local stakeholders must be reviewed or authorised by the Clerk where it is publicly shared. Routine messaging or internal operational use does not require prior approval.

11.2.5 Council-issued social media accounts, group messaging tools, or AI tools remain council property. Login credentials must be shared with the council for continuity, and accounts must be updated or deactivated when a councillor leaves office or a staff member ceases employment.

11.3 Confidentiality and data protection

11.3.1 All council-related information, including stakeholder contact details and messages, remains the property of the council and must not be transferred to personal devices or accounts without prior approval.

11.3.2 Councillors, staff, and other authorised users must comply with data protection and privacy requirements when posting or sharing information online or via messaging/AI platforms. Special category data or sensitive council information must never be shared on unapproved platforms.

11.3.3 All social media or messaging activity may be subject to monitoring under Section 7. Users should assume that public or council-related content may be retained or reviewed for compliance, security, or legal purposes.

11.4 Professional conduct and accountability

11.4.1 Councillors must observe the Members' Code of Conduct and Nolan Principles. Staff must follow council disciplinary and professional standards.

11.4.2 Users are personally responsible for the content they post or share online, including comments, images, or AI-generated material. Misuse may result in disciplinary action, legal liability, or reputational harm.

11.4.3 Media inquiries regarding council business should be referred to the Clerk.

11.4.4 Councillors, staff, and other authorised users leaving the council must delete all council-related data from personal devices, remove themselves from council-related online accounts, and ensure that AI or social media content complies with confidentiality requirements.

11.5 Misuse

Misuse of council IT systems, devices, email, social media, messaging apps, or AI tools is not in line with the council's standards of conduct and will be treated seriously. Any inappropriate or unauthorised use may result in formal action, including disciplinary proceedings, termination of engagement, or, in serious cases, dismissal.

Reviewed at Governance and Finance Committee 17th March 2026
Ratified at Full Council 25th March 2026
Due for review March 2027