

PENTON GRAFTON PARISH COUNCIL

INFORMATION TECHNOLOGY (IT) AND ACCEPTABLE USE POLICY

Adopted: ____Sept 2026____

Review Date: ____2027____

Version: 1.1

Aligned to current NALC/SAPPP Proper Practices and available HALC/NALC sector guidance on digital and data compliance.

1. POLICY STATEMENT

1.1 Penton Grafton Parish Council recognises the importance of information technology in delivering Council services, supporting decision-making, maintaining effective communication and demonstrating good governance.

1.2 The Council is committed to ensuring that information technology systems, email, websites, software, devices and information assets are used securely, responsibly and in accordance with legal requirements.

1.3 This Policy sets out standards for acceptable use of Council information technology and supports the Council's compliance with the Annual Governance and Accountability Return requirements, including Assertion 10 on digital and data compliance.

2. PURPOSE

The purpose of this Policy is to:

- Protect Council information, records and digital assets;
- Reduce cyber security risks;
- Support compliance with UK GDPR and the Data Protection Act 2018;
- Support compliance with Freedom of Information and transparency obligations;
- Promote responsible use of Council equipment, personal devices, email, websites and software;
- Ensure continuity of Council business and recoverability of key records;
- Support the Council's ability to answer AGAR Assertion 10 appropriately.

3. SCOPE

This Policy applies to councillors, employees, contractors, volunteers and any individual authorised to access Council information, systems or digital services.

The Policy applies to:

- Council-owned devices;
- Personal devices used for Council business;
- Council email accounts and any approved shared mailboxes;
- Websites and online publication platforms;
- Cloud storage and file sharing systems;
- Software applications and online services;
- Electronic records, including emails, documents, images, datasets and backups.

4. RESPONSIBILITIES

The Council

The Council shall:

- Approve and review this Policy;
- Ensure appropriate resources and arrangements are in place for secure IT use;
- Promote good information governance, cyber security and digital accessibility;
- Ensure that significant IT, cyber security and data protection risks are considered and managed.

The Clerk

The Clerk shall:

- Administer Council IT arrangements or ensure appropriate administration is in place;
- Maintain or arrange suitable security measures;
- Manage Council records in approved locations;
- Report significant IT incidents, cyber incidents and data breaches to the Council where appropriate;
- Maintain access controls and ensure access is removed promptly when no longer required;
- Ensure that Council digital records remain accessible to the Council when councillors, staff or contractors leave office or employment.

Councillors and Users

Users shall:

- Comply with this Policy;
- Protect Council information and personal data;
- Use Council systems, accounts and devices responsibly and lawfully;

- Report security incidents, suspected data breaches, lost devices and suspicious communications promptly;
- Co-operate with reasonable arrangements to preserve Council records and maintain continuity of business.

5. COUNCIL EMAIL AND DOMAIN USE

5.1 Official Council business should be conducted through approved Council email accounts wherever reasonably practicable.

5.2 The Council shall maintain a generic email account hosted on a Council-owned domain for official Council business. The official Clerk email address is clerk@pentongrafton-pc.gov.uk. The Council shall use role-based Council email addresses rather than relying on person-specific free email accounts.

5.3 Council email accounts shall be used professionally and in accordance with Council policies. Users shall not use personal email accounts as the primary means of storing or conducting Council business unless there is a specific and documented reason.

5.4 Users shall:

- Exercise care when sending emails;
- Verify recipients before sending personal, confidential or sensitive information;
- Avoid forwarding Council information to private accounts unless authorised and necessary;
- Retain email records in accordance with the Council's Document Retention and Disposal Policy;
- Ensure that Council emails remain accessible to the Council where required for business continuity, Freedom of Information requests, subject access requests, audit or governance purposes.

5.5 Where shared or role-based mailboxes are used, access shall be limited to authorised users and reviewed periodically.

6. PASSWORD SECURITY AND MULTI-FACTOR AUTHENTICATION

Users shall:

- Use strong, unique passwords or passphrases for Council systems;
- Keep passwords confidential;
- Not share passwords with others;

- Change passwords promptly where compromise is suspected;
- Use a secure password manager where approved by the Council.

Where available, multi-factor authentication shall be enabled for Council email, cloud storage, website administration and other key systems.

7. DEVICE SECURITY

Council-owned and personal devices used for Council business shall:

- Be protected by password, PIN or biometric security;
- Use up-to-date operating systems and software where reasonably practicable;
- Have anti-virus or equivalent protection where appropriate;
- Be kept secure when unattended;
- Use encryption where available and proportionate;
- Be configured to reduce the risk of unauthorised access to Council information.

Lost or stolen devices containing Council information must be reported immediately to the Clerk.

8. USE OF PERSONAL DEVICES

8.1 Councillors and staff may use personal devices for Council business where necessary, provided Council information remains secure and accessible to the Council where required.

8.2 Users must ensure that:

- Appropriate security measures are applied;
- Council information remains protected;
- Personal data is not disclosed improperly;
- Council records are not held solely on a personal device or personal account;
- Council information is removed from personal devices when no longer required or upon leaving office where appropriate.

8.3 The Council may require users to confirm that Council information has been returned, transferred or securely deleted when their role ends.

9. SOFTWARE AND CLOUD SERVICES

9.1 Only appropriately licensed and approved software shall be used for Council business.

9.2 Software updates shall be applied promptly where practical, particularly security updates.

9.3 Users shall not install unauthorised software on Council-owned devices without approval.

9.4 Cloud storage, file sharing and collaboration tools shall only be used where approved by the Council and where Council records can be retained, accessed and recovered appropriately.

10. INTERNET USE

Users shall use internet access responsibly and lawfully.

Users must not:

- Access unlawful material;
- Engage in activity that may compromise Council systems;
- Download malicious or unauthorised software;
- Use Council resources for improper purposes;
- Bypass security controls or knowingly expose Council information to unnecessary risk.

Reasonable personal use may be permitted where it does not interfere with Council business, create additional risk, or conflict with Council policies.

11. DATA PROTECTION, FOI AND TRANSPARENCY

11.1 Personal information shall be handled in accordance with UK GDPR, the Data Protection Act 2018 and the Council's Data Protection Policy.

11.2 Users shall:

- Access only information necessary for their role;
- Protect confidential and personal information;
- Use secure methods for storing and sharing personal data;
- Report suspected breaches immediately;
- Assist the Council in meeting Freedom of Information, subject access and transparency obligations.

11.3 Council records, including email and electronic documents, must be retained and retrievable where required for lawful access requests, audit, governance or transparency purposes.

12. RECORDS MANAGEMENT

12.1 Electronic records are Council records and must be retained appropriately.

12.2 Records shall be managed in accordance with:

- The Document Retention and Disposal Policy;
- Freedom of Information legislation;
- Data protection legislation;
- Transparency and audit requirements applicable to local councils.

12.3 Important Council records shall be stored in approved locations and should not be held only in individual personal accounts, personal devices or unmanaged systems.

13. WEBSITE MANAGEMENT AND ACCESSIBILITY

13.1 The Council website shall:

- Comply with legal publication requirements;
- Include and maintain an Accessibility Statement;
- Be regularly reviewed for accuracy, accessibility and security;
- Protect personal information;
- Support compliance with current accessibility standards, including WCAG 2.2 AA where applicable.

13.2 Website content shall only be published by authorised persons.

13.3 Website administration access shall be protected by strong passwords and multi-factor authentication where available.

13.4 Documents published online should be prepared in an accessible format where reasonably practicable.

14. CYBER SECURITY

The Council shall seek to protect its information through:

- Secure passwords and multi-factor authentication;
- Timely software updates;
- Anti-virus or equivalent protection where appropriate;
- Secure backups;
- User awareness and vigilance;
- Appropriate access controls;
- Periodic review of digital risks.

Users shall remain vigilant against:

- Phishing emails;
- Fraud attempts;
- Suspicious links and attachments;

- Social engineering attacks;
- Malware, ransomware and unauthorised access attempts.

15. BACKUP AND BUSINESS CONTINUITY

15.1 Important electronic records shall be backed up where reasonably practicable.

15.2 The Council shall seek to ensure that key governance, financial, statutory and operational records remain recoverable.

15.3 Recovery arrangements shall be reviewed periodically, including arrangements for access if a councillor, employee or contractor is unavailable or leaves their role.

16. INCIDENT REPORTING

Users must immediately report:

- Data breaches or suspected data breaches;
- Cyber security incidents;
- Lost or stolen devices;
- Suspected unauthorised access;
- Malware infections;
- Suspicious emails, links or attachments affecting Council systems.

The Clerk shall maintain records of significant incidents and report matters to the Council, insurers, police, the Information Commissioner's Office or other relevant bodies where appropriate.

17. MONITORING

17.1 The Council reserves the right to monitor and manage its systems where necessary to:

- Protect Council information;
- Investigate suspected misuse;
- Ensure compliance with legal obligations;
- Maintain business continuity and system security.

17.2 Monitoring shall be proportionate, lawful and carried out in accordance with applicable legislation and Council policies.

18. NON-COMPLIANCE

Failure to comply with this Policy may result in:

- Removal or restriction of access to Council systems;
- Investigation by the Council;
- Referral to relevant authorities where appropriate;
- Disciplinary, contractual or code of conduct action where applicable.

19. REVIEW OF POLICY

19.1 This Policy shall be reviewed:

- Annually;
- Following significant cyber security incidents;
- Following legislative, regulatory or proper-practice changes;
- Following audit recommendations;
- Following material changes to Council IT systems, website arrangements or email provision.

19.2 Any amendments shall be approved by resolution of Penton Grafton Parish Council.

ADOPTION

This Information Technology (IT) and Acceptable Use Policy was adopted by Penton Grafton Parish Council at a meeting held on:

Date: ___ Sept 2026_____

Minute Reference: ___0926/7_____

Chairman's Signature: ___P Foster_____

Clerk's Signature: ___H Easton_____