

Information Technology (IT) Policy

January 2026, David de Niese

1. Purpose in Relation to AGAR Returns

The 2025 Edition of the Annual Governance and Accountability Returns (AGAR) for financial years commencing on or after 1 April 2025 introduced Assertion 10 for digital and data compliance. To warrant a positive response the authority needs to have implemented an Information Technology policy covering the matters enclosed.

2. Introduction

Granborough Parish Council recognises the importance of effective, secure, and well governed information technology and email usage in supporting its statutory duties, business operations, decision making, and communications.

This policy establishes mandatory standards for the use of IT resources and email and defines clear responsibilities to ensure:

- Protection of council information and personal data
- Compliance with UK GDPR, the Data Protection Act, and other legal obligations
- Consistent, professional, and auditable communications
- Reduction of risk from loss, misuse, or unauthorised access

This policy is intentionally explicit. Lack of technical knowledge, informality, historical practice, personal preference, or use of personal equipment is not an acceptable excuse for failing to protect data or to work safely.

3. Scope

This policy applies to all individuals who use Granborough Parish Council IT resources or process council information, including:

- Councillors
- The Clerk and any employees
- Volunteers
- Contractors and third parties

It applies to:

- Council owned devices
- Personally owned devices used for council business
- Computers, laptops, tablets, mobile phones, and storage devices
- Networks, internet access, software, and cloud services
- Email accounts and electronic communications
- All personal data and council records, electronic or paper

This policy is complementary to the following Granborough Parish Council policies:

- The GPC Parish Council Privacy Notice
- The GPC Freedom of Information policy
- The GPC Information and Data Protection policy
- The GPC Data Retention policy

These policies can be found at www.granborough.org/policies-and-procedures

4. Acceptable Use of IT Resources and Email

Granborough Parish Council IT resources and email accounts are provided for official council business only.

4.1 Permitted Use

IT resources may be used for:

- Statutory and governance activities
- Council administration and communication
- Engagement with residents, partners, contractors, and regulators

Limited personal use is permitted only where it:

- Does not interfere with council business
- Does not introduce security or legal risk
- Complies fully with this policy

4.2 Prohibited Use

Users must not:

- Share accounts or passwords
- Access data beyond their authority
- Install unauthorised software
- Circumvent security controls
- Use council systems for personal disputes, campaigning, or private interests

All use must comply with ethical standards, copyright and intellectual property law, and must avoid unlawful, offensive, or inappropriate content.

4.3 No Excuse Principle

All users are expected to:

- Understand their responsibilities
- Seek advice from the Clerk or Data Protection Officer if unsure
- Act cautiously where personal or sensitive data is involved

Failure to protect council data or to work safely will be treated as a governance and compliance issue regardless of intent.

5. Device and Software Usage

Where possible, authorised devices, software, and applications will be provided by Granborough Parish Council.

5.1 Authorised Devices

Council owned devices must:

- Be used in accordance with this policy
- Be secured with passwords or biometric controls
- Be kept physically secure

5.2 Software Controls

Unauthorised installation of software on council-owned devices, including personal software, is strictly prohibited due to security and licensing risks.

Only software approved by the Clerk and / or the Data Protection Officer may be installed or used for council business on council-owned devices.

Unsupported or end of life software must not be used and will not be approved.

6. Data Management and Security

All council information must be handled lawfully, fairly, and securely.

6.1 Secure Storage and Transmission

Sensitive or confidential data must:

- Be stored only in approved systems
- Be encrypted, where required under UK law or Parish Council policies.
- Not be stored unnecessarily on local or removable media

USB drives must be encrypted or avoided.

6.2 Catalogue of Personal Identifiable Information Holders

Granborough Parish Council is a Data Controller and Data Processor.

The UK GDPR requires Granborough Parish Council to maintain records of where personally identifiable information (PII) is held. All persons in scope of this policy must inform the Data Protection Officer and the Clerk if they hold any PII on a personal (BYOD) device because of their role with the Council.

The Clerk must maintain a catalogue of such data and the reasons for it being held and processed by users.

6.3 Backups and Recovery

All council data essential to governance, finance, statutory compliance, and service delivery must be backed up and retained in accordance with the Granborough Parish Council Data Retention Policy, including:

- Financial and accounting records
- Council email accounts
- Minutes, agendas, and governance documents
- Personal data and trust fund records where applicable

Backups must:

- Be taken at least monthly by the Data Protection Officer or Clerk
- Be automated where possible
- Be encrypted and protected from unauthorised access
- Include at least one copy stored separately from the primary system

Restore testing must be carried out at least annually and evidence retained.

The Clerk is responsible for ensuring backups are taken monthly, and for ensuring backups are effective. Given the technical nature of these activities, these responsibilities can be delegated, but the clerk remains accountable.

7. Network and Internet Usage

Granborough Parish Council networks and internet connections must be used responsibly and efficiently for official purposes only.

Users must not:

- Download or share copyrighted material without authorisation
- Access unlawful or inappropriate content
- Introduce security risks through unsafe browsing or downloads

8. Email Communication

8.1 Mandatory Use of Authority Owned Email Accounts

All official council business must be conducted using Granborough Parish Council owned or approved email accounts. This includes:

- Correspondence with residents and the public
- Communications with contractors, auditors, and regulators
- Internal council discussions and decision making
- Transmission of documents containing personal data

Use of personal email accounts for council business is not permitted.

8.2 Limited Exception

Personal email may only be used for Council business where:

- The communication is transferred promptly to the council email system, and
- The Clerk and Data Protection Officer are informed

8.3 Standards of Communication

Emails must be:

- Professional, accurate, and respectful
- Written on the assumption they may be disclosed
- Consistent with the council's legal and governance obligations

Sensitive information must not be sent unless encrypted.

Users must be vigilant against phishing, malware, and suspicious links or attachments, given the risks this poses to the broader Granborough IT estate.

8.4 Record Keeping

Council email accounts are the official record of communications and must not be used to obscure, delete, or avoid record keeping obligations.

9. Password and Account Security

Users are responsible for maintaining the security of their accounts.

Requirements include:

- Strong, unique passwords with a minimum length of 12 characters and use of letters, numbers, and special characters
- No sharing of passwords
- Multi factor authentication, where available
- Prompt reporting of suspected compromise
- Passwords must not be written down or reused across services.

10. Mobile Devices and Remote Work

Mobile devices used for council business must:

- Be secured with passcodes or biometric authentication
- Auto lock after inactivity
- Have a supported and recent (within 1 year) operating system installed.
- Use device-level encryption

Use of personal devices under BYOD does not reduce responsibility. If a device cannot meet these standards, it must not be used.

11. Email Monitoring

Granborough Parish Council reserves the right to monitor email communications and IT usage to ensure:

- Compliance with the GPC policies, including this policy
- Protection of council systems and data
- Compliance with legal and regulatory obligations

Monitoring will be proportionate and conducted in accordance with UK GDPR and the Data Protection Act 2018.

12. Retention and Archiving

Emails and records must be retained and archived and retained in accordance with legal and regulatory requirements, and the GPC Data Retention Policy.

Users must:

- Retain records required for governance, audit, or statutory purposes
- Make use of Council-owned Microsoft 365 and OneDrive accounts for storage
- Avoid unnecessary duplication
- Dispose of data securely and irreversibly when no longer required

More information on retention periods and archiving can be found within the GPC Data Retention Policy, which is considered the authority for these topics.

Users must not:

- Use non-approved Cloud services for retention and archiving, such as Dropbox, Google Drive, Apple iCloud, and Box
- Retain Council information longer than defined in the Data Retention policy
- Keep copies of emails and documents outside approved systems
- Delete, destroy, or alter Council information subject to a legal hold, audit, FOI request, or investigation.
- Dispose of Council information without using approved secure deletion or destruction methods.

13. Reporting Security Incidents

All suspected or actual incidents must be reported immediately to the Clerk and to the Data Protection Officer.

This includes:

- Loss or theft of devices
- Unauthorised access
- Malware or phishing incidents
- Accidental disclosure of personal data

Incidents will be logged, assessed with the Data Protection Officer, and escalated where required, including notification to the ICO within statutory timeframes.

14. Training and Awareness

Granborough Parish Council will provide appropriate training and guidance on:

- IT security
- Data protection responsibilities
- Email and communication standards

The Clerk is responsible for arranging the above training, and for ensuring that new councillors and staff are briefed on this policy.

15. Compliance and Consequences

Failure to comply with this policy may result in:

- Removal of access to council systems
- Mandatory corrective action or training
- Referral to regulators or other authorities where required

16. Policy Review

This policy will be reviewed at least annually, or sooner following:

- A significant incident
- Changes in law or guidance
- Material changes to council systems or operations

17. Contacts and Oversight

Operational responsibility:

- Clerk and Responsible Financial Officer

Data protection oversight:

- Data Protection Officer

All councillors, staff, and contractors are individually responsible for protecting Granborough Parish Council's IT systems, email, and data.

The Clerk will ensure a standing agenda item on IT and Data Protection Compliance will be included at least quarterly, including confirmation of recent backups and any issues, which must be recorded in the minutes

Policy Acknowledgement and Compliance Sign Off

I confirm that I have read, understood, and agree to comply with the Granborough Parish Council Information Technology (IT) Policy.

I understand that:

- I am personally responsible for protecting council information and personal data
- Official business must be conducted using council owned email accounts
- Failure to comply may result in removal of access or further action

Name: _____

Role: _____

Signature: _____

Date: _____