



GISLINGHAM PARISH COUNCIL

IT & LAPTOP POLICY

Policy Overview:

Gislingham Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications. This policy outlines guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

Scope

This policy applies to all individuals who use any Gislingham Parish Council Parish Council IT resources, including (where provided):

- computers
- networks
- software and applications
- devices
- data storage
- email accounts

Acceptable Use of IT Resources and Email

Council IT resources and email accounts are to be used for official council-related activities and tasks.

Limited personal use is permitted, provided it:

- does not interfere with work responsibilities
- does not breach this policy
- remains lawful and appropriate

Users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Device and Software Usage

Where possible and proportionate, authorised devices may be provided.

Gislingham Parish Council Parish Council **does not currently provide any authorised devices.**

Software and applications provided by third parties for installation on personal devices should be used only for work-related tasks.

Unauthorised installation of software on any authorised device (if provided in future), including personal software, is strictly prohibited due to potential security risks.

Data Management and Security

All sensitive and confidential council data is stored in applications and cloud platforms provided by third-party suppliers. These systems store and transmit data securely using approved methods.

Regular data backups are provided by third-party suppliers to guard against data loss, and secure data destruction methods are used when necessary.

Network and Internet Usage

Gislingham Parish Council does not currently provide dedicated network or internet connections.

If provided in future, they must be used responsibly and efficiently for official purposes. Downloading or sharing copyrighted material without proper authorisation is prohibited.

Email Communication

.gov.uk email accounts provided by a third party for Gislingham Parish Council are for official communications only.

Users must ensure that:

- emails are professional and respectful
- confidential or sensitive information is not sent unless encrypted
- attachments and links are treated with caution
- the source of unexpected emails is verified before opening links or files

Password and Account Security

Users are responsible for maintaining the security of their accounts and passwords.

Councillors are advised to:

- create strong passwords of at least 8 characters including upper/lower case letters, numbers, and symbols
- use two-factor or biometric authentication where available
- create a distinct password for council email accounts or cloud storage
- consider using a passphrase of 4–5 memorable but random words

Password strength can be safely tested here:

<https://www.grc.com/haystack.htm>

Mobile Devices and Remote Work

Mobile devices are not currently provided by the council.

If supplied in future, they must be secured with passcodes and/or biometric authentication.

When working remotely, users must follow the same security practices as if working in an office.

Gislingham Parish Council currently has **no office premises**.

Email Monitoring

The council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws.

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

Retention and Archiving

Emails should be retained and archived in accordance with legal and regulatory requirements.

Reporting Security Incidents

All suspected security breaches or incidents must be reported immediately to the Parish Clerk, the designated IT point of contact.
This includes any email-related security incidents or suspicious activity.

Training and Awareness

The council may provide training and resources to educate users about IT security best practice, privacy concerns, and technology updates.
All employees and councillors are asked to read the appendix on best practices and awareness.

Compliance and Consequences

Breaches of this IT and Email Policy may result in the suspension of accounts and access to parish council email and shared areas.

Policy Review

This policy will be reviewed annually to ensure its relevance and effectiveness.

Contacts

For IT-related enquiries or assistance, users should contact the **Parish Clerk**.
All staff and councillors are responsible for the safety and security of the council's IT and email systems.

Additional Note

A laptop that is the property of the Parish Council must **never** be used for other employment or personal use.

Signed: *CFell* Chair

Approved by Gislingham Parish Council on 20th July 2026

Date of next review July 2027