

Information Technology (IT) Policy

1. Purpose and Scope

This policy sets out how Hethersgill Parish Council will use, manage, and protect its information technology (IT) systems and digital assets. It applies to all councillors, employees, volunteers, contractors, and anyone else authorised to access council systems and data.

The policy covers all forms of information and communication technologies including council-owned devices, email systems, websites, cloud storage, third-party platforms, and personal devices used for council business.

This IT Policy should be used alongside the council's other adopted policies and procedures. Together, these documents form the council's approach to responsible digital governance and legal compliance.

2. Roles and Responsibilities

The **Clerk** is responsible for managing this policy and ensuring IT resources are used appropriately and securely.

Councillors and **staff** are responsible for complying with the policy and reporting any breaches or incidents immediately.

All external **IT support providers** and **contractors** must adhere to the standards set out in this policy when handling council information.

3. Acceptable Use

IT systems and council-issued devices must only be used for legitimate council business. Personal use is discouraged when council issued devices are available. The use must not interfere with work responsibilities or compromise the council's security or reputation.

The use of personal email accounts for council business is prohibited. All council correspondence must be conducted through official council email addresses.

Under no circumstances should non-public meetings or conversations be recorded without the permission of all present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

4. Data Security and Confidentiality

All devices used to access council data must be password-protected. Where possible, two-factor authentication should be enabled for cloud-based systems and emails. This is to support compliance data protections under GDPR and the Data Protection Act 2018.

Documents containing personal data or sensitive information must be stored securely, preferably in encrypted cloud-based storage. Any transfer of such data must use secure sharing tools including secure emails.

Consent must be obtained before sharing any personal information including email addresses. If consent is not obtained, any correspondence / documents these must be anonymised before sharing.

Staff and councillors must not disclose confidential council information to any unauthorised person, either during or after their term of office or employment.

5. Software and Hardware Management

Only authorised software approved by the Clerk or IT support provider may be installed on council devices. Updates and security patches must be regularly applied.

All staff and councillors accessing council information must make sure the devices being used are safe to use by being up to date with all updates and security.

Obsolete or faulty equipment must be securely wiped before disposal, and hardware must be disposed of in line with environmental regulations.

6. Email and Communication Standards

All official communications must use the council's designated email system. Emails must be professional, respectful, and concise, and must not contain defamatory or offensive material.

Email accounts must include a standard disclaimer regarding data protection and information requests.

Consent must be obtained before sharing any personal information including email addresses. If consent is not obtained, any correspondence / documents these must be anonymised before sharing.

BCC should be used when sending general information to the public.

7. Website and Social Media Governance

The council's website and any official social media accounts are managed by the Clerk or designated officers, who are responsible for ensuring published content is accurate, professional, lawful, and does not compromise the council in any way.

Any comments received via social media must be moderated in line with the council's Policy.

Websites must comply with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 and publish a valid accessibility statement.

8. Remote Working, Mobile and Personal Devices

Staff and councillors working remotely must ensure they use a secure internet connection and do not leave devices unattended in public or shared spaces. Devices must be locked when not in use and must not be shared with family members or others.

All devices used to access council data must be password protected.

Council documents should not be downloaded onto personal devices unless approved. Where possible the user should maintain a clear separation between personal data processed on the council's behalf and personal use. All documents stored relating to the personal data within the council roll should not be saved onto personal accounts as this may breach data protection legislation.

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 servers/services via their own IT equipment and users are personally liable for their own device(s) and for any costs incurred.

9. Incident Reporting and Cyber Security

Any data breach, loss of equipment, or suspected cyber incident must be reported immediately to the Clerk, who will investigate and determine whether the breach needs to be reported to the Information Commissioner's Office (ICO).

The council will follow procedures outlined in its Data Protection Policy and maintain an incident log.

All councillors and staff must remain vigilant against phishing attempts and other online threats.

10. Training and Awareness

All new councillors and employees will receive the IT and data protection policies during induction. GDPR and IT safety training will be offered to all with additional periodic refresher training offered.

Staff and councillors are encouraged to familiarise themselves with National Cyber Security Centre (NCSC) guidance on staying safe online.

11. Compliance with Legislation

This policy ensures compliance with:

- Local Government Act 1972
- Freedom of Information Act 2000
- Data Protection Act 2018 and the UK General Data Protection Regulation
- Local Audit and Accountability Act 2014
- Public Sector Bodies Accessibility Regulations 2018
- Local Government Transparency Code 2015
- Electronic Communications Act 2000

Council data and IT practices will be reviewed regularly to ensure compliance with these and other relevant regulations.

12. Disaster Recovery and Backup

The Clerk must ensure that critical council documents and emails are backed up at least weekly using a secure and encrypted cloud-based service. Backup systems should include automatic version control and the ability to restore data in the event of accidental deletion or system failure.

A disaster recovery plan must be maintained and reviewed annually, including defined recovery time objectives (RTOs) and procedures for restoring essential operations.

13. Third-party Access and Security Standards

Any contractors or third-party software providers accessing council data or systems must do so under a formal agreement. This agreement must specify minimum cybersecurity standards and ensure compliance with the Data Protection Act 2018.

Access must be limited to the data or systems necessary for their role, logged appropriately, and revoked as soon as work is completed.

15. Digital Inclusion and Accessibility

The council recognises the importance of digital inclusion. Support and training will be offered to councillors and staff who are less confident using technology. Residents who are digitally excluded will be offered alternative methods of accessing council information and services, such as paper notices or telephone enquiries.

The council's website and online documents must comply with accessibility regulations and offer downloadable content in accessible formats.

16. Review and Monitoring

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

Breaches of this policy may result in disciplinary action, reporting to the Monitoring Officer, or other action in line with the council's Code of Conduct or HR procedures.

This policy supports the council's commitment to maintaining high standards of transparency, accountability, and information security.

This policy will be reviewed annually by the Clerk and presented to the full council for approval.

— policy ends here —

Contact Details

Please contact us if you have any questions about this policy or complaints at:
Clerk, Hethersgill Parish Council, School House, Low Row, Brampton, CA8 2LN

Email: clerk@hethersgillparish.gov.uk

Accepted by FCM and Adopted: DATE

Date for next review: DATE

Review: Annually

Amendment Notes -

Date accepted by FCM	Amendment

DRAFT