Hartpury Parish Council

IT Policy

Adopted: 2nd March 2026

Reviewed 4th May 2026

Scope

This policy sets the expectations for management, protection and appropriate use of IT equipment and systems provided by Hartpury Parish Council. It applies to all Councillors, Staff, Volunteers and other authorised users.

The policy covers all IT systems including Council owned devices, email systems, websites, cloud storage and personal devices used for Council business. The policy works alongside all Council policies and procedures to ensure Digital and Data compliance.

Roles and Responsibilities

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

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

External IT support providers and contractors must adhere to the standards set out in this policy when handling Council information.

Acceptable Use

IT systems and email accounts provided by the Council must be used for official Council related work only.

Any hardware or devices provided by the Council may be allowed limited personal use provided it does not interfere with work responsibilities or violate any part of this policy.

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

Personal email accounts should not be used for Council business; all emails should be sent and received through the Council provided email addresses.

Device (Hardware) and Software Management

Any hardware provided by the Council should be regularly checked for updates and security patches, these must be installed where available. Unauthorised installation of software on a Council owned

device is prohibited to reduce security concerns. If a device becomes faulty or obsolete this should be reported to the Clerk immediately for the correct action to be taken. Any faulty or obsolete hardware should be securely wiped and disposed of in the correct manner, considering environmental regulations.

Data Security

Any device used to access council data (including emails) should be password protected. Where possible two-factor authentication should be used for Cloud based systems and emails.
Users are responsible for the security of their accounts and devices; passwords should be strong and kept confidential.
Documents containing personal data or other sensitive information should preferably be kept in encrypted cloud-based storage. Any transfer of personal data or sensitive information must use secure sharing methods.
Councillors and Staff must not disclose any confidential information to any unauthorised person at any time, during or after their term of office or employment.

Remote Working and Mobile Devices

Staff and Councillors working remotely must use a secure internet connection. Devices must not be left unattended in public or shared spaces. Devices must remain locked when not in active use and must not be shared with others.
Council documents must not be downloaded onto personal devices without authorisation from the Clerk.

Email Communications

Email communications must be sent using the Council provided email accounts. Emails must be professional, respectful, and concise, and must not contain defamatory or offensive material.
Attachments must not be opened unless you can verify the source to ensure security. If an unverified attachment is opened and any concerns over phishing or malware are raised, you must inform the Clerk immediately.
Confidential and sensitive information must not be sent via email without prior authorisation and must be suitably encrypted before sending.
Emails should be kept in line with the Council's retention policy.

Website and Social Media

The Council's website is managed by the Clerk, who is responsible for ensuring content is accurate, lawful and updated regularly.
The Council does not currently have any Social Media accounts.
Websites must comply with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 and publish a valid accessibility statement.

Accessibility and Digital Inclusion

The Council understands the importance of digital inclusion and accessibility; they are committed to ensuring that everybody can access Council information.

Support and training can be provided to any Councillors and Staff who are less confident with technology.
Residents who are unable to access digital contact can be offered alternative methods to access information such as paper copies and telephone enquiries.
All documents on the Council website will be provided in an accessible format and will comply with accessibility regulations.

Backup and Recovery
The clerk must ensure that critical Council documents and emails are backed up regularly, preferably to 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 a system failure.

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.

Third-party Access and Security
Any contractors or third-party software providers that access Council data or systems mist do so under formal agreement. The agreements must specify minimum security standards required and ensure compliance with the Data Protection Act 2018.
Access in these instances must be limited to the data and systems necessary to carry out the role and be revoked as soon as work is completed.

Training and Awareness
All Councillors and employees are encouraged to familiarise themselves with National Cyber Security Centre (NCSC) Guidance on staying safe online.
IT and Data Protection training will be offered to all Councillors and employees upon starting their role. Periodic refresher training will also be offered. All staff and Councillors are encouraged to participate in Data Protection training. Staff who are responsible for processing Personal Data on behalf of the Council will be required to complete Data Protection training.

Compliance with Legislation
This policy ensures compliance with the following legislation:

- 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 regularly reviewed to ensure continued compliance with the above and any additional relevant legislation.

Compliance with this Policy

Compliance with this Policy is mandatory, any breaches of this policy will likely result in disciplinary action for staff or reporting to the Monitoring Officer for Councillors. Other actions in line with the Code of Conduct may also be taken.

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

Review and Monitoring

This policy will be reviewed yearly by the Clerk and presented for approval.

The Clerk will monitor changes to legislation throughout the year, should it be required any necessary changes will be made and bought to Council at the earliest opportunity.