HEDLEYHOPE PARISH COUNCIL

IT Policy

1. Introduction

Hedleyhope Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy sets out the guidelines and responsibilities for the appropriate use of IT resources and email and ensures that council information is handled securely and responsibly in line with data protection laws.

2. Scope

This policy applies to all councillors, employees and contractors who use or manage the parish council's IT resources, including email accounts, council data, the council website and personal devices used for council business.

3. Council Email Accounts

Each councillor and the Clerk has a council-provided email address which must be used for all council business.

Requirements:

- Email accounts should only be used for council-related communication.
- Personal email accounts must not be used for council business.
- No emails or council data or documents from council-owned accounts should be forwarded to personal email addresses.
- Confidential or sensitive information must not be sent via email unless it is encrypted.
- Emails relating to council business are considered council data and may be subject to disclosure under the Data Protection Act or Freedom of Information Act.
- Emails should be retained and stored in compliance with the UK GDPR, Data Protection Act and Freedom of Information requirements. Regularly review and delete unnecessary emails.
- Appropriate password security should be maintained. Email passwords should not be shared with others and should not be used on personal accounts. Log out of shared devices after use.
- Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

Access control:

When a councillor leaves office, the Clerk will remove access to council email.

4. Use of Personal Devices (Bring Your Own Device – BYOD)

Personal devices include mobile phones, tablets, laptops and desktop computers. When accessing council information on personal devices, users must ensure that reasonable security measures are in place.

Devices used for council work must:

- Be protected by a password, PIN, or biometric lock.
- Have automatic screen locking enabled.
- Use up-to-date operating systems and software.
- Have security updates installed regularly.
- Use antivirus software where available.

Devices should not be used for council business if they are compromised, infected with malware, or shared in an unsecured way.

Council data must be kept separate from personal data using dedicated storage areas.

Removable media such as USB drives should be encrypted or password protected when containing sensitive council information.

On leaving the council, councillors and employees must delete any council information stored on personal devices where appropriate.

5. Parish Council Website

The parish council maintains an official website. The Clerk manages the website on a day-to-day basis and is responsible for:

- Uploading agendas, minutes and documents.
- Ensuring information is accurate and up-to-date.
- Ensuring personal data is not published unnecessarily.
- Complying with transparency and accessibility requirements.
- Ensuring that the website is secure.

Website content should reflect official council decisions and information.

Audits for website accessibility and link functionality will be carried out every six months.

6. Data Protection and Security

Hedleyhope Parish Council recognises its role as both a data controller and data processor. All processing of personal data will comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. All data collection, processing and subject rights are governed by the council's Data Protection and Privacy Policies. Personal data is stored securely and is retained in accordance with the council's Data Retention Policy.

7. Backup and Data Retention

Council digital records are stored securely and backed up regularly to two external hard drives accessed by the Clerk. Records that are no longer required are permanently deleted from all storage devices and backups in accordance with the council's Data Retention Policy.

8. Security and Data Breaches

Any suspected security issue or data breach must be reported to the Clerk as soon as possible.

Examples include:

- Loss or theft of a device containing council information.
- Unauthorised access to council email accounts.
- Accidental sharing of confidential information.
- Malware or suspected hacking.

The Clerk will assess the issue and take appropriate action in line with the council's Data Protection Policy and UK GDPR requirements.

9. Policy Review

This policy will be reviewed annually by the council to ensure its relevance and effectiveness, or sooner if required due to changes in technology, legislation, or council practices.