HELPRINGHAM PARISH COUNCIL

IT POLICY

Adopted: 11/2/26
Minute ref: 162/26
Review: Jan 2027

1. Purpose

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

This policy outlines the principles governing the use of IT systems, email, and electronic information when acting on behalf of the Council and applies to the use of personally owned devices and systems used for Council business aswell as any Council owned IT equipment.

2. Scope

This policy applies to all councillors, employees, volunteers, and contractors who use IT systems, devices, or email to carry out HPC business, whether using personal or third-party equipment and services.

3. General Principles

All users must:

- Use IT systems and email responsibly, lawfully, and for legitimate Council purposes
- Comply with relevant legislation, including the Data Protection Act 2018 and UK GDPR
- Protect the confidentiality, integrity, and availability of Council information
- Avoid actions that could expose the Council to data loss, security breaches, or reputational damage

4. Acceptable Use

HPC IT resources and email accounts are to be used for official council related activities and tasks. Limited incidental personal use is permitted provided it does not interfere with Council duties, incur costs, or breach this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

5. Devices and Software

Authorised devices, software, and applications may be provided by HPC for work-related tasks. Any device, personal or owned by HPC which is used for Council business must:

- Be protected by appropriate security measures (e.g. passwords, PINs, biometric access)
- Have up-to-date operating systems and security software
- Prevent unauthorised access to Council information

Software or applications used for Council business must be reputable and lawful. Users must not install or use software that could compromise security or data protection.

6. Information and Data Security

Council information must be stored and transmitted securely using approved methods. Where personal devices are used for Council business it must be ensured that:

- Council data is kept separate where possible
- Data is not shared with unauthorised individuals

- Council information is deleted securely when no longer required or when the user ceases to act on behalf of the Council

7. Email and Electronic Communications

Email accounts used for HPC business must be used professionally and appropriately. Users must:

- Ensure emails are accurate, respectful, and suitable for public disclosure
- Avoid sending confidential or sensitive information unless appropriate safeguards (e.g. encryption) are in place
- Remain vigilant against phishing, malware, and suspicious links or attachments

8. Passwords and Access Control

- Users are responsible for maintaining the security of passwords and account credentials used for Council business.
- Passwords must be strong, kept confidential, and not shared. Where possible, multi-factor authentication should be used.

9. Remote Working and Mobile Access

When accessing Council information remotely or via mobile devices, users must apply the same standards of security as if working in a controlled office environment. Devices must not be left unattended or accessible to unauthorised persons.

10. Monitoring and Privacy

HPC reserves the right, where lawful and proportionate, to monitor the use of IT systems and email used for Council business to ensure compliance with this policy and legal obligations. Any monitoring will be conducted in accordance with data protection legislation.

11. Records Retention

Electronic records and emails relating to Council business are Council records and must be retained, archived, or deleted in line with the Council's retention policies and legal requirements.

12. Security Incidents

Any actual or suspected IT security incident, data breach, or loss of Council information must be reported immediately to the Clerk, who will take appropriate action in line with the Council's data protection procedures.

13. Training and Awareness

HPC will promote appropriate guidance and training to support good cyber security practice. Users may be directed to authoritative sources such as the National Cyber Security Centre: https://www.ncsc.gov.uk/collection/phishing-scams

14. Breaches of Policy

Failure to comply with this policy may result in restricted access to Council systems and other action deemed appropriate by the Council.

15. Review

This policy will be reviewed annually by HPC and updated as necessary to reflect changes in legislation, guidance, or working practices.

16. Responsibility

All councillors and staff share responsibility for safeguarding Helpringham Parish Council's information and electronic communications. Compliance with this policy supports transparency, accountability, and good governance.