

# Great Haseley Parish Council IT Policy

## **1. Introduction**

Great Haseley 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 the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

## **2. Scope**

This policy applies to all individuals who use Great Haseley Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

## **3. Acceptable use of IT resources and email**

Great Haseley Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

## **4. Device and software usage**

Where possible, authorised devices, software, and applications will be provided by Great Haseley Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

## **5. Data management and security**

All sensitive and confidential Great Haseley Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

## **7. Email communication**

Email accounts provided by Great Haseley Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

## **8. Password and account security**

Great Haseley Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

## **9. Email monitoring**

Great Haseley Parish Council reserves the right to monitor parish council email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

## **10. Retention and archiving**

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

## **11. Reporting security incidents**

All suspected security breaches or incidents should be reported immediately to the Parish Clerk for investigation and resolution and if appropriate the Information Commissioners Office (ICO). Report any email-related security incidents or breaches to the Parish Clerk.

## **12. Training and awareness**

Great Haseley Parish Council will encourage Councillors and the Parish Clerk to attend training about IT security best practices, privacy concerns, technology updates along with email security and best practices.

## **13. Compliance and consequences**

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

## **14. Policy review**

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

## **15. Contacts**

For IT-related enquiries or assistance, users can contact the Parish Clerk.

The Parish Clerk and Councillors are responsible for the safety and security of Great Haseley Parish Council's IT and email systems. By adhering to this IT and Email Policy, Great Haseley aims to create a secure and efficient IT environment that supports its mission and goals.

Date: 9<sup>th</sup> March 2026

Signature:  **REDACTED**

Role: Chairman, Great Haseley Parish Council

