East Hagbourne Parish Council

IT Policy

1. Introduction

East Hagbourne 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. This policy should be read in conjunction with the parish council's Data Protection & Information Governance Policy, which sets out the legal requirements for handling personal data.

2. Scope

This policy applies to all individuals who use East Hagbourne parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

East Hagbourne parish council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, 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.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by East Hagbourne parish council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

If using your own device you must make sure you use strong passwords for all your accounts, download the latest operating system security updates, and use anti-virus software.

5. Data management and security

All sensitive and confidential East Hagbourne 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. Access to data must be limited to what is necessary for each role. Personal data should not be kept on devices longer than necessary and must be securely deleted.

6. Network and internet usage

East Hagbourne parish council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited. Public Wi-Fi networks can be targeted by hackers. Always make sure you are using a trusted internet connection when carrying out official business.

7. Email communication

Email accounts provided by East Hagbourne 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. Any FOI or Subject Access Requests must be forwarded promptly to the Parish Clerk.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links. Do not download and open anything if you are unsure who has sent it.

8. Social Media

East Hagbourne parish council may use social media (such as Facebook) as an official communication channel. Only the Clerk or persons authorised by the council may post on official Council accounts. All content must be lawful, factual, politically neutral and consistent with formally agreed Council decisions. Confidential, personal or

commercially sensitive information must not be disclosed. Login details for official Council social media accounts shall be held by the Clerk.

Councillors using personal social media accounts must clearly distinguish between personal views and statements made in an official capacity and must comply at all times with the Council's Code of Conduct.

The Council may operate informal electronic messaging groups (such as WhatsApp) for the purpose of information sharing only. Where a group is quorate, care must be taken to ensure there is no decision-making outside of properly convened meetings.

9. Password and account security

East Hagbourne 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. For business continuity, login details should be stored securely so they can be accessed in an emergency.

10. Mobile devices and remote Work

Mobile devices provided by East Hagbourne parish council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office. Where personal devices are used, Council data must be kept secure and deleted when no longer required.

11. Email monitoring

East Hagbourne parish council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. If you are using a personal account for council business, this is still subject to data protection laws and FOI requests. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

12. 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.

13. Reporting security incidents

All suspected security breaches or incidents must be reported immediately to the Parish Clerk. Incidents involving personal data will be handled in line with the Data Protection and Information Governance Policy.

14. Training and awareness

East Hagbourne parish council will provide information on accessible training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will be encouraged to undertake regular training on email security and best practices.

15. Compliance and consequences

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

16. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

17. Contacts

For IT-related enquiries or assistance, users can contact parishclerk@easthagbourne.net

All staff and councillors are responsible for the safety and security of East Hagbourne parish council's IT and email systems. By adhering to this IT Policy, East Hagbourne parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Date: 16 April 2026

Signature: P. Dixon

Role: Vice Chair, presiding the meeting