GLEMSFORD PARISH COUNCIL
INFORMATION TECHNOLOGY (IT) POLICY

1. Introduction

Glemsford Parish Council recognises the importance of effective and secure information technology (IT), including email and social media usage, in supporting its business operations and communications, and the need to safeguard the Council's digital data and assets.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources, email and social media by council members, employees, volunteers, and contractors.

2. Scope

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

3. Acceptable use of IT resources, email and social media

Glemsford Parish Council IT resources email and social media 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. Check accuracy and confidentiality of information and copyright of photos before sharing, as inappropriate comments and postings can adversely affect the reputation of the council. Posting on the council's social media page is only to be carried out by the designated administrator/s.

4. Device and software usage

Where relevant, authorised devices, software and applications will be provided by Glemsford parish council for work-related tasks. A database of equipment will be kept. 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 Glemsford 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.

6. Network and internet usage

Glemsford 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.

7. Email communication

All councillors and employees who need to use email as part of their role will normally be given their own email address and account on a domain owned by the council. Email accounts provided by the council are for official communication only. Emails should be professional and respectful in tone. The council may, at any time, withdraw email access should it feel that it is no longer necessary for the role or if the system is being abused.

All councillors, staff and other authorised users should 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

Glemsford Parish Council email users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong, such as using three random words, and not shared with others. Regular password changes are encouraged to enhance security.

9. Mobile devices and remote work

Mobile devices provided by Glemsford 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.

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 email-related security incidents or other security breaches should be reported immediately to the designated IT point of contact, the Parish Clerk, for investigation and resolution. Where a security breach affects personal data, the council will follow the guidance in its Data Protection Policy.

12. Training and awareness

The Parish Clerk will advise councillors and staff of relevant training resources and opportunities, including those offered through the county association (SALC), relating to email security, best practices, privacy concerns and technology updates.

13. Compliance and consequences

Breach of this IT 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. Updates may be made to address emerging technology trends and security measures.

15. Contacts

For IT-related enquiries or assistance, users can contact Glemsford Parish Clerk. All staff and councillors are responsible for the safety and security of Glemsford parish council's IT systems. By adhering to this IT Policy, Glemsford parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Policy adopted: March 2026