GREAT WALTHAM PARISH COUNCIL

Information Technology (IT) Policy

Version 1

This policy document should be reviewed and updated as necessary

Version	Review Date	Reviewed By	Summary of Changes
1	October 2025	S. Gilbert	New document.

Great Waltham Parish Council – Information Technology (IT) Policy

1. Introduction

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

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

2. Scope

This policy applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, and data. Resources include access to .gov.uk email addresses and any associated digital storage.

3. Acceptable use of IT resources

The Council's IT resources, where provided, are to be used for official council-related activities and tasks. Personal use should be limited and should not interfere with the Council's 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 appropriate and possible, authorised devices, software, and applications will be provided by the 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 Council data should be stored and transmitted securely using approved methods. Measures should be implemented to ensure appropriate regular data backups are performed to prevent data loss, and secure data destruction methods should be used when necessary. Confidential and sensitive data should be reviewed at regular intervals and where appropriate deleted in accordance with previously agreed destruction dates (in particular those specified in the Council's Document Retention Policy).

6. Network and Internet usage

The 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

Email accounts provided by the Council are for official communication only and their use should incorporate email signatures. Emails used to transact Council business should be professional and respectful in tone. Whenever possible, confidential or sensitive information must not be sent by email unless it is encrypted. If email encryption is not available alternative

secure methods of communication may be appropriate for confidential and sensitive material. (See Appendix for guidance on confidential information).

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

   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. Mobile devices and remote work

   Mobile devices provided by the Council should be secured with passcodes and/or biometric authentication.

10. Email monitoring

    The Council reserves the right to monitor email communications on accounts provided by the Council to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Other emails used to transact Council business must comply with all Council policies (in particular its Document Retention Policy) and any GDPR requirements.

11. Retention and archiving

    Email accounts provided by the Council should be retained and archived in accordance with legal and regulatory requirements. Users should regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

    All suspected security breaches or incidents should be reported immediately to the Parish Clerk for investigation and resolution.

13. Training and awareness

    The Council will provide resources to educate users about IT security best practices, privacy concerns, and technology updates. Completion of IT training and awareness provided by the Council will be recorded in members and employees training records.

14. Compliance and consequences

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

15. 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.

16. Contacts

For council IT-related enquiries or assistance, users can contact in the first instance, the Parish Clerk.

All staff and councillors are responsible for the safety and security of the Council's IT resources. By adhering to this IT policy, the Council aims to create a secure and efficient IT environment that supports its functions.

Appendix

Guidance on confidential information

There is no legal definition of "confidential information" that is of general application. The confidentiality or otherwise of information therefore needs to be considered in the context of individual circumstances. However, by way of general indicative guidance, the following categories of information would normally be treated as confidential:

a) All reports, briefing notes and other documents or communications issued by the Council or Council members that are marked confidential.

b) Matters concerning details of commercial negotiations.

c) Where there is a legal restriction on the disclosure of information (for example under the Data Protection Act, contractual obligations, a court order or pending legal proceedings covered by the sub judice rule).

d) Matters concerning terms and conditions of employment of individual officers or pending grievance or disciplinary proceedings.

e) Personal information concerning individual service recipients.

f) Information which, given its nature, timing and context is such that a reasonable person would consider it to be confidential. (This would, for example, normally be the case when information is supplied to a member by the Parish Clerk, a fellow councillor, or another person and is clearly stated to be confidential). The disclosure of such information would normally tend to have a detrimental effect on the interests of the Council, the service users or third parties involved.

Some information which would otherwise be confidential may nevertheless be subject to public rights of access under the law. This, for example, would include subject access under the Data Protection Act 1998, a specific request for access under the Freedom of Information Act 2000, access to accounts and records under the Audit Commission Act 1998, as well as access to meetings and documents under the Local Government Act 1972. Such rights may be general or limited to a "qualifying" individual. Some rights of access to information also have procedural requirements attached to them (such as the need to submit the request in writing). It is therefore generally advisable for such requests to be forwarded to the Parish Clerk, even where the member may have the information at his/her disposal.

It is not necessary for a person who supplies information to have stated expressly that the information is confidential. For example, the fact that correspondence is not marked "confidential" does not necessarily stop it from being confidential. Often the fact that the information is confidential may be inferred from the subject matter and the surrounding circumstances. If Council members or employees believe the material is confidential or they "ought reasonably to be aware of" the confidential nature of the information, it must be treated as such.