Thwing & Octon Parish Council – IT Policy

Adopted: 13.10.2025

Review: Annually or sooner if required

1. Introduction

Thwing & Octon Parish Council recognises the importance of secure and effective information technology (IT) and email usage in supporting its business, operations, and communications.
This policy sets out the rules and responsibilities for the use of council IT equipment, systems, and email accounts by councillors, the Clerk, and any contractors or volunteers acting on behalf of the Council.

2. Scope

This policy applies to all individuals who use the Council's IT resources, including laptops, software, cloud services, mobile devices, email accounts, and any other digital systems managed by or on behalf of the Council.

3. Email Use

- The Clerk will use the official clerk@ email address for all council business.
- Councillors must use a dedicated email address solely for council business, separate from any personal accounts.
- Personal email accounts must not be used for council business.
- All council emails should be professional, respectful, and stored securely.

4. Devices

- The Clerk uses a parish-provided laptop, which is password-protected.
- Councillors may access their council email accounts on personal devices, provided those devices are password-protected, regularly updated.
- Unauthorised software must not be installed on council devices.

5. Data Storage & Backup

- Council data is stored primarily on the parish laptop and secure cloud storage approved by the Council.
- Regular backups are maintained to prevent data loss.
- Wherever possible, the Council avoids keeping unnecessary paper records, relying on secure digital copies instead.

6. Mobile Phone Use

- The Clerk may use a personal mobile phone to receive parish-related calls.
- No personal data will be stored on the device beyond essential contact details required for communication.

7. Data Protection & GDPR

- This IT Policy must be read in conjunction with the Council's Data Protection Policy and Information Asset Register (Data Map).
- All IT and email use must comply with UK GDPR and the Data Protection Act 2018.

8. Freedom of Information & Records Management

- Emails and electronic records form part of the Council's official records and may be subject to Freedom of Information (FOI) and Environmental Information Regulations (EIR).
- Data must be retained and disposed of in line with the Council's Retention and Disposal Schedule.

9. Password & Account Security

- Users are responsible for maintaining the security of their council accounts.
- Passwords must be strong, not shared, and updated regularly.
- Accounts must be locked when devices are unattended.

10. Incident Reporting

- Any suspected IT security incident or data breach must be reported immediately to the Clerk.
- The Clerk will investigate and, if necessary, report to the Information Commissioner's Office (ICO) within 72 hours as required by law.

11. Training & Awareness

- Councillors and staff will be offered training on GDPR, cyber security, and safe use of IT and email systems.
- The Council will provide updates when new risks or best practices arise.

12. Compliance & Enforcement

- Breach of this policy may result in suspension of IT privileges and further action by the Council as deemed appropriate.
- In serious cases involving data breaches, the matter may be reported to the ICO.

13. Policy Review

This policy will be reviewed annually, or sooner if required by changes in legislation, best practice, or technology used by the Council.