Dalton Parish Council IT Policy

1. Purpose

This IT Policy sets out how digital devices, systems, and information are to be used securely and lawfully by the Parish Council. It applies to the Parish Clerk (the sole employee) and all councillors.

The aim of the policy is to: - Protect council information and personal data - Ensure compliance with data protection legislation - Promote safe and appropriate use of IT - Support transparency and good governance

2. Scope

This policy applies to: - All councillors - The Parish Clerk - All council-owned IT equipment - Personal devices used for council business

3. Council Email and Accounts

- Council business must be conducted using council-provided email accounts hosted on the council's official domain.
- Personal email accounts must not be used for council business, except in exceptional circumstances.
- Login details must be kept secure and not shared.

4. Acceptable Use of IT

Users must: - Use IT systems only for legitimate council business - Take reasonable steps to prevent unauthorised access - Not install unauthorised software or apps on council devices - Not access, store, or transmit inappropriate or unlawful material

5. Use of Personal Devices

- Dalton Parish Council does not provide devices for Councillors. Therefore, Councillors may use personal devices for council business.
- Personal devices used for council business must be protected by a password, PIN, or biometric security.
- Council information must not be shared with unauthorised individuals.
- Users must take care when accessing council data on public or unsecured networks.

6. Data Protection and Confidentiality

- All users must comply with data protection legislation, including UK GDPR and the Data Protection Act 2018.
- Personal data must be processed lawfully, fairly, and securely.
- Council information should only be retained for as long as necessary and in line with retention guidance.

- Any suspected data breach must be reported immediately to the Parish Clerk (or the Chair if the Clerk is affected).

7. Security Measures

- Strong passwords must be used and changed when advised.
- Devices should be locked when not in use.
- Anti-virus and security updates should be kept up to date.
- Council data should be backed up where appropriate.

8. Website and Accessibility

- The council website must meet WCAG 2.2 AA accessibility standards where reasonably practicable.
- Documents published online should be accessible and regularly reviewed.

9. Training and Awareness

- Councillors and the Clerk should have a basic awareness of IT security and data protection responsibilities.
- Guidance and support will be provided as necessary.

10. Breaches and Misuse

- Failure to comply with this policy may result in action being taken by the council.
- Serious breaches may be reported to the appropriate authority.

11. Review

This policy will be reviewed at least every two years, or sooner if there are changes to legislation or council arrangements.

Adopted by Dalton Parish Council: 12th January 2026

Next review due: Annual Meeting 2028