IT & Information Security Policy

Version: 1.0
Date Adopted: Trialled 2025 -2025. Final version approved 13/04/2026
Review Date: 12/04/2027
Responsible Officer: Clerk to the Council

---

1. Purpose

This policy sets out how Davenham & Bostock Parish Council manages and protects its information, systems, and technology. It ensures:

- Secure handling of council information
- Compliance with legal and regulatory requirements
- Clear responsibilities for councillors and staff
- Protection of the Council's reputation and assets

This policy was formally adopted by Davenham & Bostock Parish Council at a meeting held on [insert date], in accordance with the Council's governance procedures.

2. Scope

This policy applies to:

- All councillors
- Council employees
- Contractors or third parties accessing council systems

It covers all devices, systems, and data used for council business.

3. Roles and Responsibilities

3.1 The Council

- Approves and reviews this policy

3.2 The Clerk (Responsible Officer)

- Acts as the lead for IT and information governance
- Manages access to systems and data
- Ensures appropriate security measures are in place

- Acts as first point of contact for incidents and breaches

3.3 Councillors and Users

- Must comply with this policy and supporting guidance
- Must handle council information securely
- Must report incidents or concerns promptly

4. Acceptable Use

Council IT systems must be used primarily for official council business.

Users must not:

- Use council systems for unlawful or inappropriate purposes
- Share confidential information without authority
- Install unapproved software

Limited personal use is permitted where it does not:

- Interfere with council duties
- Breach security requirements
- Damage the council's reputation

5. Devices and Access

5.1 Devices

- Council-issued devices are preferred
- Personal devices may only be used with approval from the Clerk
- All devices must be password-protected and kept secure

5.2 Access Control

- Access to systems (including IONOS email and website services) is granted by the Clerk
- Access must be based on role and necessity
- Accounts must not be shared
- Access will be revoked when no longer required

6. Passwords and Authentication

- Passwords must be strong and unique
- Multi-factor authentication (MFA) must be enabled where available (including IONOS services)

- Passwords must not be shared or stored insecurely

7. Information Security

7.1 Data Classification

Information should be treated as:

- Public
- Internal
- Confidential

Confidential data must be handled with additional care.

7.2 Storage

- Council data must be stored in approved systems (IONOS email accounts and any council-approved storage platforms)
- Data must not be stored on unapproved personal devices or media

7.3 Sharing

- Use council email accounts hosted via IONOS
- Apply password protection to sensitive files where appropriate
- Share only with authorised recipients

8. Data Protection

The Council will comply with all applicable data protection legislation.

Users must:

- Only collect necessary personal data
- Keep data accurate and secure
- Not retain data longer than necessary
- Report any suspected data breach immediately to the Clerk

9. Incident Management

An incident includes:

- Loss or theft of a device
- Suspected data breach
- Phishing or cyber attack

All incidents must be reported immediately to the Clerk.

The Clerk will:

- Assess the incident
- Take appropriate action
- Escalate where required

10. Cybersecurity

Users must:

- Be alert to phishing and suspicious emails
- Not open unknown attachments or links
- Keep devices updated with security patches

11. Remote Working

When working remotely:

- Use secure networks
- Avoid public Wi-Fi unless using secure access
- Prevent unauthorised viewing or discussion of council matters

12. Backup and Retention

- Council systems must ensure appropriate backups (as provided by IONOS or other approved services)
- Records must be retained in line with the Council's retention schedule
- Users must not delete records prematurely

13. Leaving the Council

When a user leaves:

- Access to systems will be removed (including IONOS accounts)
- Council equipment must be returned
- Council data must be handed over or deleted from personal devices

14. Compliance and Monitoring

Failure to comply with this policy may result in:

- Removal of access to systems

- Formal action by the Council

15. Related Policies

This policy should be read alongside:

- Data Protection Policy
- Standing Orders
- Code of Conduct
- Records Retention Policy (if adopted)

16. Review

This policy will be reviewed annually or when required due to changes in legislation or technology.

Version Control

Version	Date	Changes	Approved By
1.0	13/04/2026	Initial version	Davenham & Bostock Parish Council