

DALTON WITH NEWTON TOWN COUNCIL

INFORMATION TECHNOLOGY, CYBER SECURITY AND INFORMATION GOVERNANCE POLICY

Policy Adopted:

Review Date:

1. Purpose

The Council recognises the importance of protecting its information, data, computer systems and electronic records.

This policy establishes the controls necessary to reduce the risk of cyber incidents, data loss, unauthorised access and service disruption.

2. Scope

This policy applies to:

- Town Councillors;
- Employees;
- Contractors and volunteers with access to Council systems;
- Council-owned devices and systems;
- Personal devices used for Council business.

3. Legal Framework

The Council will comply with:

- Data Protection Act 2018;
- UK General Data Protection Regulation (UK GDPR);
- Freedom of Information Act 2000;
- Local Government Transparency requirements;
- Current edition of the Practitioner's Guide for Smaller Authorities.

4. Roles and Responsibilities

Council

The Council is responsible for ensuring adequate resources and controls are in place to protect information and IT systems.

Clerk/RFO

The Clerk is responsible for:

- Day-to-day management of Council IT systems;
- Managing user access;
- Maintaining backups;
- Reporting data breaches where required;
- Monitoring compliance with this policy.

Councillors and Staff

Users are responsible for:

- Protecting Council information;
- Following security procedures;
- Reporting security incidents immediately.

5. Information Security Principles

Information shall be:

- Kept confidential where required;
- Accurate and reliable;
- Available to authorised users when needed;
- Protected from unauthorised access, alteration or loss.

6. Access Controls

- Access shall be restricted to authorised users.
- User accounts must not be shared.
- Access permissions shall reflect operational need.
- Access shall be removed promptly when employment or office ends.

7. Passwords and Authentication

All Council systems must be protected by secure passwords.

Where available, Multi-Factor Authentication (MFA) should be enabled.

Passwords must:

- Not be shared;
- Be unique to the system used;

- Be changed immediately if compromise is suspected.

8. Council Email and Cyber Awareness

Users must:

- Exercise caution when opening links and attachments;
- Remain alert to phishing attempts;
- Verify unexpected requests involving payments or banking details;
- Report suspicious emails immediately.

9. Council Equipment

Council-owned devices must:

- Be password protected;
- Have current operating system updates installed;
- Have antivirus protection enabled where applicable;
- Be locked when left unattended.

Loss or theft of equipment must be reported immediately.

10. Personal Devices

Personal devices used for Council business must:

- Be secured by password, PIN or biometric protection;
- Be kept up to date;
- Store Council information securely.

Confidential Council information should not be stored on personal devices unless authorised.

11. Data Storage and Retention

Council information shall be stored in approved locations.

Access to personal data shall be restricted to authorised persons.

Records shall be retained and disposed of in accordance with the Council's Retention Policy.

12. Backups

The Council shall maintain regular backups of important electronic records.

Backup arrangements should:

- Reduce the risk of data loss;
- Support business continuity;
- Be reviewed periodically.

13. Artificial Intelligence (AI)

Artificial Intelligence tools may be used to assist with administrative tasks such as drafting, summarising or research.

Users must not upload confidential, personal, commercially sensitive or legally privileged information into publicly available AI systems unless appropriate safeguards are in place.

All AI-generated content must be reviewed by a human before use.

Responsibility for decisions and published content remains with the Council and its officers.

14. Data Breaches and Security Incidents

Any actual or suspected:

- Data breach;
- Cyber attack;
- Loss of equipment;
- Unauthorised disclosure of information;
- Security incident;

must be reported to the Clerk immediately.

The Council will investigate incidents and report them to the Information Commissioner's Office where legally required.

15. Remote Working

When working remotely, users must:

- Protect confidential information;
- Avoid leaving devices unattended;
- Ensure information cannot be viewed by unauthorised persons;
- Take reasonable precautions when using public networks.

16. Procurement of IT Systems

Before introducing new software, cloud services or IT systems, the Council shall consider:

- Security arrangements;
- Data protection compliance;
- Backup arrangements;
- Supplier reliability;
- Business continuity implications.

17. Monitoring and Compliance

The Council reserves the right to monitor use of its systems where lawful and necessary to:

- Protect Council assets;
- Investigate security incidents;
- Ensure compliance with Council policies.

18. Review

This policy shall be reviewed annually or sooner where significant changes occur in legislation, technology or cyber security risks.

Signed

Chair

Minute Number.....