Cresswell Parish Council

Information Technology, Digital and Data Management Policy

(Including AGAR Assertion 10 Compliance)

1. Introduction

Cresswell Parish Council recognises the importance of maintaining secure, reliable and transparent digital systems in order to carry out its statutory duties and provide effective services to the community.

This policy establishes how the Council manages:

- Information technology systems
- Digital communications
- Electronic records
- Data protection and privacy
- Cyber security risks

The policy reflects good practice guidance issued by the National Association of Local Councils and the Society of Local Council Clerks and supports compliance with Assertion 10 within the Annual Governance Statement of the Annual Governance and Accountability Return (AGAR).

2. Purpose

The purpose of this policy is to ensure that:

- Council information is protected from loss, misuse or cyber attack
- IT systems are used appropriately and securely
- Personal data is processed lawfully
- Digital communications are properly managed

- The Council complies with audit and governance requirements

This policy supports the Council's compliance with AGAR Assertion 10, which requires smaller authorities to demonstrate appropriate arrangements for digital and data management.

3. Scope

This policy applies to:

- All Parish Councillors
- The Parish Clerk / Responsible Financial Officer
- Council employees
- Contractors acting on behalf of the Council
- Any individual accessing Council information systems

It covers:

- Computers and mobile devices used for Council business
- Email systems
- Council websites and digital platforms
- Cloud storage systems
- Electronic documents and records
- Personal devices used for Council work

4. Responsibilities

Council

The Parish Council is responsible for:

- Approving this policy

- Ensuring appropriate governance arrangements exist
- Monitoring compliance with digital and data management standards

Parish Clerk

The Parish Clerk is responsible for:

- Day-to-day administration of Council IT systems
- Maintaining a record of Council IT assets
- Managing access to digital systems
- Ensuring appropriate backups are undertaken
- Reporting any cyber security incidents or data breaches

5. Council Email and Digital Communications

To support transparency, accountability and audit compliance, Council business should be conducted through Council-controlled email accounts.

The Council will seek to ensure:

- Councillors and staff use official Council email addresses where available
- Council communications can be retained and retrieved for governance purposes
- Records of Council correspondence are maintained appropriately

Where personal email accounts are used temporarily for Council business, relevant messages must be retained as Council records.

6. Acceptable Use of IT Systems

Council IT systems must be used responsibly and primarily for Council business.

Users must:

- Protect Council information and systems

- Maintain confidentiality where required
- Comply with Council policies and legal obligations

Users must not:

- Install unauthorised software
- Share passwords with others
- Use Council systems for personal commercial purposes
- Access or distribute illegal or inappropriate material

Limited personal use may be permitted provided it does not interfere with Council business.

7. Cyber Security

The Council will take reasonable steps to protect its systems and information.

These may include:

- Anti-virus and anti-malware software
- Regular system updates
- Secure password requirements
- Multi-factor authentication where available
- Secure storage of electronic data
- Routine data backups

Users must immediately report suspicious emails, cyber threats or possible security incidents to the Clerk.

8. Data Protection

The Council processes personal data in accordance with the:

- UK General Data Protection Regulation
- Data Protection Act 2018

Personal data must be:

- Processed lawfully and fairly
- Collected for legitimate Council purposes
- Stored securely
- Retained only as long as necessary

Any suspected data breach must be reported to the Clerk immediately.

9. Storage and Backup of Data

Council information should be stored within approved systems to ensure security and continuity.

The Council will aim to:

- Store documents within secure cloud or controlled digital storage systems
- Avoid storing official records solely on personal devices
- Maintain regular backups of important Council data
- Ensure information can be retrieved for audit and governance purposes

10. Use of Personal Devices

Councillors or staff using personal devices for Council work must ensure that:

- Devices are protected by passwords or other security measures
- Software and security updates are installed regularly
- Council data is stored securely
- Council information can be retrieved if required

Council information must be removed from personal devices when an individual leaves office or employment.

11. Website and Online Information

The Council website should provide accessible and up-to-date information about Council activities.

Where possible the Council will ensure that:

- Statutory information is published
- Documents such as agendas, minutes and financial information are available
- Online information is accurate and maintained regularly

12. Records Management

Electronic records form part of the Council's official records and must be retained in accordance with the Council's Records Retention Policy.

Records may be required for:

- Internal and external audit
- Legal compliance
- Public access requests
- Transparency obligations

Users must not delete Council records unless permitted by the retention schedule.

13. Training and Awareness

The Council will encourage appropriate training for councillors and staff relating to:

- Cyber security awareness

- Data protection responsibilities
- Safe use of IT systems

Training opportunities may be available through the Society of Local Council Clerks or other recognised providers.

14. Breach of Policy

Failure to comply with this policy may result in:

- Removal of access to Council IT systems
- Investigation by the Council
- Disciplinary action where applicable

Serious breaches may be reported to relevant authorities.

15. Review of Policy

This policy will be reviewed:

- Annually
- When legislation or national guidance changes
- Following any significant cyber security incident

Adoption of Policy

This policy was adopted by Cresswell Parish Council at a meeting of the Council held on:

Date: _____

Minute Reference: _____

Signed:

Chair of the Council

Parish Clerk