Carlton Scroop and Normanton Parish Council:

IT Policy

Date of adoption: 16/03/26

Minute reference: 20260316 - 13.1

Proposed and Seconded by councilors: Proposed by Councillor England, seconded by Councillor Thomas

Chair of the Council: Alan Thomas

Clerk / Responsible Financial Officer: Florence Hill

1. Introduction

Carlton Scroop and Normanton Parish Council henceforth known as “The Authority” recognises the importance of effective, secure and lawful use of information technology (IT) and email systems in supporting its statutory duties and communications.

This policy should be read in conjunction with:

- The Authority’s **Privacy Notice**
- The Authority’s **Data Retention Policy**
- The Authority’s **Data Breach Procedure**

The Privacy Notice explains how personal data is collected, used, stored and protected by the Authority. This IT Policy sets out the technical and behavioural rules that support those commitments.

The Authority stores all Council documents electronically using a secure, password-protected Google Drive account. Access to this Google Drive is strictly limited to the Clerk and the Chair.

The Authority operates a password-protected Council email account. Access to this account is restricted to the Clerk and the Chair only.

This policy ensures compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990

2. Scope

This policy applies to:

- All councillors
- The Clerk and Responsible Financial Officer
- Volunteers
- Contractors handling Council data

It covers the use of:

- Council IT systems
- Council email accounts
- Cloud storage (Google Drive)
- Personal devices used for Council business

All users must comply with this policy to ensure the Authority meets the data protection commitments outlined in its Privacy Notice.

3. Training and Awareness

The Authority will source appropriate cybersecurity and data protection guidance to ensure users understand their responsibilities.

Users are encouraged to engage with training resources including:

- The Parish Council Domain Helper Service virtual cybersecurity workshops
- The National Cyber Security Centre small organisation guidance and Cyber Action Toolkit

Training supports compliance with the Authority's Privacy Notice and legal data protection duties.

4. Acceptable Use of IT Resources and Email

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

Users must:

- Act professionally and responsibly
- Respect confidentiality of personal data
- Follow the data handling principles set out in the Privacy Notice
- Use Council systems in a lawful and ethical manner

Limited personal use is permitted provided it does not:

- Interfere with Council duties
- Breach data protection law
- Incur cost to the Authority
- Compromise security

5. Secure Storage and Access Controls

In accordance with the Authority's Privacy Notice:

- All Council electronic documents are stored on a secure, password-protected Google Drive.
- Access to Google Drive is restricted to the Clerk and the Chair.
- The Council email account is password protected and accessible only to the Clerk and the Chair.

No Council data should be stored on unauthorised cloud services or personal storage platforms.

Access permissions are reviewed when office holders change to ensure continued data security and business continuity.

6. Use of Personal Devices

Where personal devices are used for Council business:

- Strong, unique passwords must be used
- Devices must be kept up to date with operating system and security updates
- Anti-virus software must be installed and active
- Council data must not be permanently stored on personal devices

Any temporary downloads of Council documents must be deleted after use.

These requirements support the secure processing commitments outlined in the Privacy Notice.

7. Network and Internet Security

Users must access Council systems only via secure, trusted internet connections.

When working remotely:

- Avoid using unsecured public Wi-Fi
- Log out of systems after use
- Ensure devices are not accessible to unauthorised persons

These measures help preserve the confidentiality and integrity of personal data.

8. Password and Account Security

Passwords must:

- Be strong and unique
- Not be shared
- Be changed immediately if compromise is suspected

Multi-factor authentication (MFA) should be enabled where available.

Login details must be securely recorded for business continuity purposes and accessible only to authorised office holders in emergencies.

9. Email Management and FOI Compliance

Council correspondence must be conducted via the official Council email account wherever possible to ensure:

- Transparency
- Proper record retention
- Compliance with the Freedom of Information Act 2000

Emails relating to Council business may be subject to:

- Freedom of Information requests
- Subject Access Requests under UK GDPR

Users must carefully check recipients before sending confidential information and remain vigilant against phishing attempts.

10. Data Management and Retention

Data must be:

- Collected only where necessary
- Stored securely on approved systems
- Retained in accordance with the Authority's retention schedule
- Deleted or destroyed securely when no longer required

These requirements directly support the Authority's Privacy Notice and UK GDPR accountability obligations.

11. Reporting Security Incidents and Data Breaches

All suspected incidents must be reported immediately to the Clerk, including:

- Loss or theft of devices
- Unauthorised access to Google Drive
- Email compromise
- Accidental disclosure of personal data

Incidents will be assessed in accordance with the Authority's Data Breach Procedure and, where required, reported to the Information Commissioner's Office within statutory timeframes.

12. Monitoring

The Authority reserves the right to access and review Council systems where necessary to:

- Ensure compliance
- Respond to legal requests
- Investigate suspected breaches

Monitoring will be proportionate and carried out in accordance with data protection legislation and the Authority's Privacy Notice.

13. Compliance and Consequences

Failure to comply with this policy may result in:

- Removal of access to Council systems
- Disciplinary action (where applicable)
- Referral to relevant authorities
- Legal reporting obligations being triggered

All users are personally responsible for ensuring compliance with data protection and cybersecurity requirements.

14. Policy Review

This policy will be reviewed annually or sooner if required due to:

- Legislative changes
- Technological developments
- Changes in Council operations

It will be reviewed alongside the Privacy Notice to ensure consistency and ongoing GDPR compliance.