

IT & INFORMATION SECURITY POLICY

ADOPTED MARCH 2026

1. Introduction

1.1 Cornsey Parish Council recognises the importance of secure and effective use of information technology in supporting council business.

1.2 This policy sets out the arrangements in place to protect council data, systems and communications and to ensure compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Local Government transparency requirements

1.3 This policy supports the Council's Data Protection Policy and forms part of its overall governance framework.

2. Scope

2.1 This policy applies to:

- The Clerk and all other employees
- All Councillors
- Any contractor or person acting on behalf of the Council

2.2 It covers:

- Personal devices used for council business
- Email systems
- Dropbox file storage
- Website management (names.co.uk)
- Data access and remote working

3. IT

3.1 The Council does not own IT equipment. Council business is conducted using personal devices.

3.2 The Council uses:

- A .org.uk domain email account (Clerk)
- A generic council email account
- Dropbox for electronic document storage
- names.co.uk for website hosting

3.3 The Clerk is responsible for administration of these systems.

4. Acceptable Use

4.1 IT systems and email accounts must be used for official council business only.

4.2 The designated council email address should be used for council correspondence wherever possible.

4.3 Council information must not be stored on unapproved platforms or shared via personal messaging apps unless unavoidable and subsequently recorded appropriately.

4.4 Users must not access, store, or transmit inappropriate, unlawful or offensive material using council systems.

5. Personal Devices (Bring Your Own Device – BYOD)

As the Council does not provide devices:

5.1 Any personal device used for council business must:

- Be protected by a strong password or biometric lock
- Have up-to-date operating system and security updates installed
- Have antivirus software where appropriate
- Automatically lock when not in use

5.2 Council data stored temporarily on personal devices must be transferred as soon as practicable.

5.3 Council data must be deleted from personal devices when no longer required.

5.4 When a councillor leaves office, they must permanently delete all council data from personal devices and confirm this to the Clerk.

6. Passwords and Account Security

6.1 Passwords must be strong and unique.

6.2 Passwords must not be shared with unauthorised persons.

6.3 Where available, two-factor authentication (2FA) must be enabled.

6.4 The Clerk will maintain secure administrative control of council email and Dropbox accounts.

7. Data Storage and Backup

7.1 Dropbox is the Council's primary electronic storage system.

7.2 Access permissions will be restricted to authorised users only.

7.3 The Clerk will ensure:

- Appropriate folder structure
- Controlled access rights
- Regular checks of user access

7.4 Dropbox's built-in version history provides document recovery capability.

7.5 Important financial and governance documents should also be retained in accordance with the Council's Document Retention Policy.

8. Email Security

8.1 Council email accounts must be used professionally and respectfully.

8.2 Users must:

- Be vigilant against phishing emails
- Avoid opening suspicious attachments or links
- Verify unusual financial requests independently

8.3 Sensitive personal data should only be sent by email where necessary and with appropriate care (e.g., password-protected attachments).

9. Website Management

9.1 The Council website is hosted by names.co.uk.

9.2 Access to website administration must be password-protected and restricted to authorised persons.

9.3 The website must comply with:

- Accessibility regulations
- Transparency Code requirements
- Data protection legislation

9.4 Personal data must not be published unless lawful to do so.

10. Data Breaches and Security Incidents

10.1 Any suspected data breach, cyber incident, or loss of council data must be reported immediately to the Clerk.

10.2 The Clerk will assess the incident and, where required, report it to:

- The Information Commissioner's Office (ICO)
- The Council's insurer

10.3 All breaches will be documented in accordance with the Data Protection Policy.

11. Remote Working

As council business is conducted remotely:

11.1 Users must ensure devices are not visible to unauthorised persons.

11.2 Public Wi-Fi should be avoided for accessing sensitive information unless a secure connection is used.

12. Retention and Disposal

12.1 Electronic records will be retained in line with the Council's Document Retention Policy.

12.2 When accounts are closed or access removed, data will be securely transferred or deleted.

12.3 Password access will be changed when personnel change.

13. Training and Awareness

13.1 Councillors should be aware of:

- Basic cyber security principles
- Phishing awareness
- Their responsibilities under data protection law

13.2 The Clerk will keep up to date with sector guidance (e.g., NALC, SLCC).

14. Monitoring and Compliance

14.1 The Council reserves the right to review its IT systems to ensure compliance with this policy and legal obligations.

14.2 Failure to comply with this policy may result in:

- Withdrawal of access to council systems
- Referral under the Members' Code of Conduct where appropriate

15. Policy Review

This policy will be reviewed annually or following any significant change in technology, legislation or council structure.