Blockley Parish Council

Data Security Policy for Councillors and Staff

Minute Ref: 20.11.25.11.1

1. Introduction

This Data Security Policy outlines the responsibilities of all councillors and staff of Blockley Parish Council (the 'Council') regarding the secure handling of personal data and Council information. All councillors and staff must read, understand, and comply with this policy as part of their role.

2. Purpose

The purpose of this policy is to:

- Ensure compliance with the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Protect the personal data of residents and members of the public
- Safeguard Council information and systems
- Minimise the risk of data breaches
- Establish clear responsibilities for data security

3. Scope

This policy applies to all councillors and staff of Blockley Parish Council, including temporary staff, volunteers, and contractors with access to Council data.

4. General Principles

All councillors and staff agree to:

- Process personal data only for the purposes for which it was collected
- Keep personal and sensitive information confidential
- Share information only with authorised individuals on a need-to-know basis
- Take reasonable steps to ensure the accuracy of data
- Retain data only for as long as necessary in line with the Council's Document Retention Policy
- Dispose of data securely when no longer required

5. Secure Handling of Physical Documents

Councillors and staff will:

- Keep all documents containing personal data secure at all times
- Store physical documents with personal data in locked cabinets when not in use
- Not leave documents containing personal data unattended on desks or in public areas
- Use a 'clean desk' approach at the end of each working day
- Transport documents securely when taking them off-site
- Shred or securely dispose of documents containing personal data when no longer needed

6. Electronic Data Security

Councillors and staff will:

- Use strong, unique passwords for all Council accounts and devices
- Use 2FA / MFA for all Council systems (if available)
- Use a password manager to save passwords, for example, Dashlane
- Change passwords regularly and never share them with others
- Lock computers and devices when unattended
- Not download or install unauthorised software on Council devices
- Ensure all devices have up-to-date antivirus or security software for example MalwareBytes
- Back up important data regularly

7. Email and Communication Security

Councillors and staff will:

- Use only Council email accounts for Council business
- Check email recipients carefully before sending to prevent accidental disclosure
- Use blind carbon copy (BCC) when sending emails to multiple recipients
- Not forward or send sensitive information via email unless necessary and secure
- Be alert to phishing attempts and report suspicious emails
- Password-protect sensitive documents when sharing electronically
- Use secure methods for sharing large files or sensitive information, for example, https://send.tresorit.com

8. Mobile Devices and Remote Working

When working remotely or using mobile devices, councillors and staff will:

- Keep devices physically secure at all times
- Use password/PIN protection and enable automatic screen locking
- Not access sensitive data on public Wi-Fi networks without using a VPN
- Report lost or stolen devices immediately
- Not store Council data on personal devices unless properly secured
- Ensure family members or others cannot access Council information

9. Data Breach Reporting

Councillors and staff will:

- Report any actual or suspected data breach immediately to the Parish Clerk
- Document the circumstances of any breach
- Cooperate fully with any investigation into a data breach
- Not attempt to hide or cover up any data security incidents

10. Training and Awareness

Councillors and staff will:

- Complete data protection training upon joining the Council – click here [external link / gov.uk]
- Attend refresher training at least annually
- Stay informed about data protection best practices
- Ask for guidance when uncertain about data protection requirements

11. Compliance and Monitoring

- The Parish Clerk will monitor compliance with this policy
- Regular audits of data security practices may be conducted
- The policy will be reviewed annually and updated as necessary
- Cllr. John will advise on best practices and assist the Parish Clerk in all matters related to cybersecurity.

Last reviewed by Cllr John 15th October 2025