Carlton Scroop and Normanton on Cliffe Parish Council:

Data Breach Procedure

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

Data Breach Procedure

1. Purpose

This procedure outlines the steps to be followed in the event of a suspected or confirmed data breach involving personal or sensitive data held by the Council.

It ensures:

- Rapid containment and assessment of breaches
- Compliance with the UK GDPR and Data Protection Act 2018
- Clear responsibilities and escalation procedures
- Proper documentation and reporting

This procedure complements the Council's Privacy Notice and IT Policy.

2. Scope

This procedure applies to all data processed or stored by the Council, including:

- Personal data of residents, staff, contractors, and councillors
- Council records stored on the secure Google Drive
- Emails and attachments stored in the Council email account
- Paper records

It applies to all councillors, staff, volunteers, and contractors with access to Council data.

3. Definition of a Data Breach

A data breach may include, but is not limited to:

- Accidental or unlawful destruction, loss, or alteration of personal data
- Unauthorised access to or disclosure of personal data
- Loss or theft of devices containing Council data
- Cyberattacks, ransomware, or phishing incidents

4. Immediate Actions

1. Contain the Breach
    - Isolate compromised systems or devices if possible
    - Prevent further unauthorised access
2. Notify the Clerk (or Chair if the Clerk is unavailable) immediately
    - Provide details of the suspected breach
    - Include the type of data involved, number of individuals affected, and any suspected cause
3. Preserve Evidence
    - Do not delete files or emails related to the incident
    - Take screenshots or notes to document what occurred

5. Assessment

The Clerk (or Chair) will:

- Determine the type and sensitivity of data involved
- Identify individuals or parties affected
- Evaluate the likely risk to the rights and freedoms of data subjects
- Decide whether containment and corrective action are sufficient

6. Reporting

1. Internal Reporting
    - Document the incident in the Council's Data Breach Log
    - Include date, time, description, assessment, and corrective action
2. External Reporting (to ICO)

    - If the breach is likely to result in a risk to individuals' rights and freedoms, the Information Commissioner's Office must be notified within 72 hours of discovery
    - Include:
        - Nature of the breach
        - Categories and approximate number of affected individuals
        - Likely consequences
        - Measures taken to mitigate impact
3. Notification to Individuals
    - If the breach is likely to result in high risk to individuals, affected parties must be informed without undue delay
    - Provide clear advice on what they can do to protect themselves

7. Corrective Actions

The Clerk (with the Chair where appropriate) will:

- Secure or recover lost data
- Reset passwords or revoke access if necessary
- Apply software updates, patches, or malware removal
- Review processes and training to prevent recurrence

8. Documentation

All breaches must be fully recorded, whether or not they require ICO notification. The record should include:

- Date and time of discovery
- Description of the breach
- Data involved and affected individuals
- Action taken to contain, report, and remedy the breach
- Lessons learned and preventive measures

This documentation ensures accountability under UK GDPR and will be reviewed during annual IT and data audits.

9. Roles and Responsibilities

- Clerk: Primary responsibility for assessing, reporting, and managing breaches
- The Data Protection Officer role will be included within the Parish Clerk's job description.
- Chair: Provides oversight and acts as secondary contact if the Clerk is unavailable

- All Users: Responsible for immediately reporting suspected breaches and cooperating with investigation

10. Training

The Council will provide:

- Regular refresher training on data protection and breach response
- Guidance on recognising phishing and other cyber threats
- Instructions for securely handling sensitive data

11. Review

This procedure will be reviewed annually alongside the IT Policy and Privacy Notice to ensure ongoing compliance and effectiveness.