Data Breach Response Policy – Lytchett Matravers Parish Council

Lytchett Matravers Parish Council

Data Breach Response Policy

1. Purpose of the Policy

This policy sets out how Lytchett Matravers Parish Council ("the Council") will respond to a personal data breach in order to comply with data protection legislation, minimise harm, and ensure prompt and effective management of incidents.

The policy supports the Council's obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Scope of the Policy

This policy applies to:

- All elected and co-opted Members of the Council
- The Parish Clerk / Responsible Financial Officer
- Any contractors or volunteers handling personal data on behalf of the Council

It applies to all personal data processed by the Council, whether held electronically or in paper form.

3. What Is a Personal Data Breach

A personal data breach is a security incident leading to the accidental or unlawful:

- Destruction of personal data
- Loss of personal data
- Alteration of personal data
- Unauthorised disclosure of personal data
- Unauthorised access to personal data

Examples include, but are not limited to:

- Loss or theft of laptops, USB drives, or paper files
- Emails sent to incorrect recipients
- Hacking, malware, or ransomware attacks
- Unauthorised access to systems or records
- Accidental deletion of personal data

4. Roles and Responsibilities

4.1 Parish Clerk

The Parish Clerk is responsible for:

- Acting as the Council's lead officer for data protection matters
- Receiving and coordinating reports of data breaches
- Assessing the severity and impact of the breach
- Maintaining a Data Breach Register
- Liaising with the Information Commissioner's Office (ICO) where required
- Informing the Council Chair as soon as practicable

4.2 Councillors, Staff, and Others

All Councillors, staff, and anyone handling Council data must:

- Take reasonable steps to prevent data breaches
- Immediately report any suspected or actual data breach to the Parish Clerk
- Cooperate fully with any investigation or remedial action

5. Reporting a Data Breach

- Any suspected or actual data breach must be reported to the Parish Clerk immediately and without delay
- Reports should include, where possible:
    - Date and time the breach occurred or was discovered
    - Description of the incident
    - Type and volume of data involved
    - Number of individuals affected
    - Any immediate actions taken

Failure to report a data breach promptly may itself be treated as a serious matter.

6. Containment and Recovery

Upon notification of a data breach, the Parish Clerk will:

- Take immediate steps to contain the breach and prevent further data loss
- Recover data where possible
- Secure systems, devices, or documents involved
- Ensure evidence is preserved for investigation

7. Risk Assessment

The Parish Clerk shall assess:

- The nature of the personal data involved (e.g. sensitive or special category data)
- The volume of data and number of individuals affected
- The likelihood and severity of risk to individuals' rights and freedoms
- Potential consequences such as identity theft, financial loss, distress, or reputational damage

The outcome of the assessment shall determine whether the breach is reportable.

8. Notification to the ICO

- Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the breach must be reported to the ICO
- Notification shall be made without undue delay and, where feasible, within 72 hours of becoming aware of the breach
- Where notification is delayed, reasons for the delay shall be recorded

9. Communication with Affected Individuals

- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those affected shall be informed without undue delay
- Communications shall be clear, transparent, and include:

- A description of the breach
- The likely consequences
- Steps taken or proposed to address the breach
- Advice on how individuals can protect themselves
- Contact details for further information

10. Recording the Breach

- All personal data breaches, regardless of severity, shall be recorded in the Council's Data Breach Register
- Records shall include:
  - Facts relating to the breach
  - Its effects
  - Remedial action taken

11. Review and Preventative Action

Following resolution of a data breach, the Parish Clerk shall:

- Review the causes of the breach
- Identify lessons learned
- Recommend changes to procedures, training, or security measures

The Council shall consider and approve any necessary improvements.

12. Training and Awareness

- Councillors and staff will be encouraged to undertake data protection training
- This policy shall be made available to all persons handling Council data

13. Breaches of This Policy

Failure to comply with this policy may result in:

- Referral to the Monitoring Officer or ICO where appropriate
- Disciplinary action in line with relevant procedures

14. Review of the Policy

This policy shall be reviewed:

- At least every four years
- Following any significant data breach
- Following changes in data protection legislation or guidance

Any amendments must be approved by the Council at a properly convened meeting.

Adopted by Lytchett Matravers Parish Council: Full Council 25th February 2026
Minute Reference: 5.3
Next Review Due: March 2029