LILBOURNE PARISH COUNCIL
Data Breach Policy & Reporting Procedure

1. Introduction
Lilbourne Parish Council ("the Council") is committed to protecting personal data and ensuring that any data breach is handled promptly, transparently, and in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
This policy applies to councillors, employees, volunteers, and contractors who handle personal data on behalf of the Council.

2. What Is a Data Breach?
A data breach is any incident that results in:
- unauthorised access to personal data
- accidental or unlawful destruction, loss, alteration, or disclosure
- personal data being unavailable when required

Examples include:
- sending information to the wrong person
- loss or theft of a laptop, phone, or USB stick
- unauthorised access to email accounts
- accidental deletion of important records
- cyber-attacks or malware infections

3. Reporting a Breach
All councillors, staff, and contractors must report suspected breaches **immediately** to the **Clerk**, providing:
- a description of the breach
- when and how it occurred
- what data may be affected
- who is involved
- any steps already taken

Delays increase risk and may result in non-compliance with the ICO's 72-hour reporting requirement.

4. Assessing the Breach
The Clerk will:
- investigate the breach
- determine what data is involved
- assess the potential impact on individuals
- decide whether the breach is likely to result in a risk to rights and freedoms

If necessary, the Clerk may consult:
- the Chair of the Council
- the Council's IT provider
- the ICO's helpline or guidance

5. Notifying the ICO
The Council must notify the ICO **within 72 hours** if the breach is likely to result in a risk to individuals.
The notification will include:
- the nature of the breach
- categories and approximate number of individuals affected
- likely consequences
- measures taken or proposed to address the breach

If the Council decides not to notify the ICO, the reasons will be documented.

6. Notifying Individuals
If the breach is likely to result in a **high risk** to individuals (e.g., identity theft, financial loss, significant distress), the Council will inform affected individuals **as soon as possible**, explaining:
- what happened
- what data is involved
- what they can do to protect themselves
- what the Council is doing to address the issue

7. Containment and Recovery
The Council will take immediate steps to:
- secure systems
- recover lost data where possible
- prevent further unauthorised access
- change passwords or access controls
- work with IT support if required

8. Record Keeping
The Council will maintain a **Data Breach Log** recording:
- date and time of breach
- nature of breach
- individuals affected
- actions taken
- whether the ICO or individuals were notified
- lessons learned

9. Review and Prevention
Following a breach, the Council will review:
- policies and procedures
- staff and councillor training needs
- security measures
- data handling practices

Improvements will be implemented promptly.

10. Contact Details
Lilbourne Parish Council Clerk: Mrs C E Valentine Email: clerk@lilbourne-pc-gov.uk
Website: www.lilbourne-pc.gov.uk

This policy is reviewed and readopted annually. Dated May 2026