Christ Church Moreton Hall

Data Breach Policy

This policy comes into effect immediately following agreement at a PCC meeting dated

27th July 2026

Purpose of This Procedure

This procedure sets out how Christ Church, Moreton Hall will identify, manage, and report personal data breaches in accordance with the UK GDPR and the Data Protection Act 2018. Its aim is to minimise harm, protect individuals' rights, and ensure compliance with legal obligations.

What Is a Data Breach?

A personal data breach is any incident that results in:

- Unauthorised access to personal data
- Unauthorised disclosure of personal data
- Loss of personal data
- Destruction or alteration of personal data
- Loss of availability of personal data

Examples include:

- Lost or stolen paper files
- Emails sent to the wrong recipient
- Unauthorised access to church computers or accounts
- Accidental deletion of important records
- Cyber-attacks or malware infections

Immediate Actions When a Breach Is Suspected

Anyone who becomes aware of a possible breach must:

1. **Report it** to the PCC Data Protection Lead or the Churchwardens, as soon as possible and at most within 24 hours
2. **Provide details**, including:
    - What happened
    - When it happened
    - What data may be affected
    - Who is involved

3. **Do not attempt to hide or fix the issue alone.**
4. For any IT related breach, immediately power down affected systems and do not switch back on until advised to do so.
5. **Preserve evidence** (emails, files, devices) without altering anything.

Containment and Assessment

The Data Protection Lead (or PCC Chair if unavailable) will:

- Assess the nature and scope of the breach
- Identify what personal data is involved
- Determine whether the data is sensitive or high risk
- Secure systems or records to prevent further loss
- Change passwords or restrict access if necessary
- Contact IT support if digital systems are affected

A preliminary assessment should be completed **within 24 hours**.

Risk Evaluation

The PCC will evaluate:

- The type and sensitivity of the data
- The number of individuals affected
- Whether individuals could suffer harm (identity theft, distress, financial loss)
- Whether the breach affects vulnerable people
- Whether the data was encrypted or protected

This assessment determines whether the breach must be reported to the ICO.

Reporting to the ICO

Once confirmed, the PCC must report a breach to the **Information Commissioner's Office (ICO)** if it is likely to result in:

- A risk to individuals' rights and freedoms
- Significant distress
- Financial loss
- Identity theft
- Reputational damage

If required, the PCC will:

- Report the breach **within 72 hours** of becoming aware of it
- Provide all required details using the ICO's reporting process

- Keep a record of the report and any correspondence

If the breach does **not** meet the threshold for reporting, the PCC will document the decision and reasons.

Informing Affected Individuals

If the breach is likely to result in a high risk to individuals, the PCC will:

- Notify affected individuals **as soon as possible**
- Explain what happened
- Describe what data was involved
- Outline steps taken to contain the breach
- Provide advice on how individuals can protect themselves
- Offer a contact point for questions

Communication should be clear, timely, and sensitive.

Documentation and Record Keeping

All breaches — whether reportable or not — must be recorded in the **PCC Data Breach Register**, including:

- Date and time of the breach
- Description of the incident
- Categories of data affected
- Number of individuals affected
- Actions taken
- Decisions about reporting
- Lessons learned

Records must be kept securely and reviewed annually.

Review and Prevention

After each breach, the PCC will:

- Review what went wrong
- Identify training needs
- Update policies or procedures
- Improve technical or organisational measures
- Report findings to the PCC at the next meeting

The aim is to prevent recurrence and strengthen data protection practices.

Responsibilities

- **PCC** — overall responsibility for data protection compliance
- **Data Protection Lead** — coordinates breach response and reporting
- **Churchwardens** — act if the Lead is unavailable
- **All volunteers and staff** — must report breaches immediately and follow this procedure