Mudford Parish Council

Data Breach Policy

This policy was adopted at the meeting of Mudford Parish Council held on 26th February 2026.

Purpose

This policy sets out how Mudford Parish Council (the council) will identify, manage and report personal data breaches in compliance with UK General Data Protection Regulations, the Data Protection Act 2018, the Freedom of Information Act 2000 and guidance issued by the Information Commissioners Office (ICO).

Introduction

Mudford Parish Council recognises its duty as a data controller to protect personal data and to respond promptly and effectively to any breach in compliance with (UK General Data Protection Regulations, the Data Protection Act 2018, the Freedom of Information Act 2000 and guidance issued by the Information Commissioners Office (ICO)).

Under Article 4(12) UK GDPR, a personal data breach is “A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.”

Examples relevant to Parish Councils include:

- Email to the wrong resident
- Loss of laptop or USB stick (staff member or councillor)
- Publication of personal data in meeting papers incorrectly
- Unauthorised access to council email accounts
- Paper files left in public view
- Website or social media publishing personal data in error

Scope

This procedure covers all personal data held by the council in electronic systems, emails, paper files and portable devices and applies to:

- The clerk and all employees
- All councillors
- All volunteers and contractors acting on behalf of the council

Roles and responsibilities
Clerk to the council (Data Protection lead)

The clerk is responsible for:

- Receiving breach reports
- Leading the breach response
- Conducting risk assessments
- Deciding on ICO notification
- Notifying affected individuals
- Maintaining the Breach Register
- Reporting serious breaches (those reported to the ICO) to the council.

The council (Corporate Responsibility)

The council will:

- Ensure appropriate polices are in place and are reviewed regularly
- Provide training
- Support remedial actions
- Review serious breaches
- Allocate resources to prevent recurrence,

Breach Response Procedure

STEP 1 – Immediate reporting
Immediately on discovery any person who becomes aware of a suspected breach MUST:

- Inform the clerk without delay
- Provide all known details
- Take immediate steps to limit the breach (if it is safe to do so)

STEP 2 – Containment and Recovery
The clerk will take urgent steps to:

- Stop or minimise the breach
- Recover disclosed information where possible
- Secure systems or documents
- Reset passwords (if necessary)
- Contact unintended recipients and request deletion
- Preserve evidence.

STEP 3 – Risk Assessment
Under articles 33 and 34 UK GDPR, the clerk will access risk to individuals' rights and freedoms considering:

- Type and sensitivity of data
- Volume of data

- Number of individuals affected
- Ease of Identification
- Potential consequences (identify theft, distress, safeguarding risk)
- Whether data was encrypted or protected

The assessment and reasoning must be documented.

STEP 4 - Notification to the ICO

Under article 33 UKGDPR and the Data Protection Act 2018 the council must notify the ICO within 72 hours of becoming aware of a breach where there is a risk to individuals rights and freedoms.