Parish Council Data Breach Policy - 2026

1 Purpose
This policy sets out how the Parish Council identifies, manages, reports, and learns from personal data breaches. It ensures compliance with:
UK GDPR
Data Protection Act 2018
ICO guidance on personal data breaches
The aim is to minimise harm to individuals, protect the Council's information assets, and maintain public trust.

2 Scope
This policy applies to:
All personal data processed by the Parish Council
All councillors, employees, volunteers, and contractors
All formats (paper, electronic, email, audio, images, website, social media, CCTV)
It covers accidental and deliberate breaches.

3 What is a Personal Data Breach?
A personal data breach is any incident that leads to:
Unauthorised access
Unauthorised disclosure
• Loss or theft
Destruction or alteration
Loss of availability
Examples include:
Sending personal data to the wrong recipient
Losing an unencrypted laptop or USB stick
Emailing documents to a personal account
Accidental deletion of key records
Website exposure of personal information
Ransomware or cyber-attack

4 Roles & Responsibilities
The Parish Council
Holds overall responsibility for compliance
Receives reports on breaches and approves corrective actions
Clerk / Responsible Officer
Acts as the Data Breach Manager
Leads breach investigation and documentation
Assesses risk and determines whether the ICO must be notified
Ensures affected individuals are informed where required
Maintains the Breach Register
Councillors, Staff, and Volunteers
Must report all suspected breaches immediately
Must not attempt to hide or resolve breaches informally
Must cooperate with investigations

5 Identifying a Breach
Any person who becomes aware of a possible breach must report it immediately to the Clerk. Delays increase risk and may breach the Council's legal duty to notify the ICO within 72 hours.
Indicators of a breach include:
Unexpected system behaviour
Missing files or unexplained deletions
Complaints from individuals
Suspicious emails or phishing attempts
Lost or stolen devices

6 Reporting a Breach
All suspected breaches must be reported using the Council's Data Breach Report Form.
Reports must include:
What happened
When and how it was discovered
What data is involved
Who is affected
Any immediate actions taken

Adopted: 3.3.26 Min 7.3 (d)

7 Containment and Recovery
The Clerk will take immediate steps to limit the impact, which may include:
Isolating affected systems
Resetting passwords
Recovering deleted data from backups
Contacting IT support
Securing physical records
Requesting return or deletion of mis-sent information

8 Assessing the Risk
The Clerk will assess:
The type and sensitivity of the data
The number of individuals affected
The potential harm (identity theft, distress, financial loss, reputational damage)
Whether the data was encrypted or protected
Whether the breach is likely to result in a risk to individuals' rights and freedoms
This assessment determines whether the ICO and affected individuals must be notified.

9 Notification Requirements
9.1 Notifying the ICO (Satswana can support you with this)
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:
Nature of the breach
Categories and volume of data affected
Likely consequences
Measures taken or proposed
Contact details for the Clerk
If the Council decides not to notify the ICO, the reasoning must be documented.

9.2 Notifying Individuals
Individuals must be informed without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
Notifications must:
Describe the breach in clear language
Explain potential impacts
Provide advice on protective steps
Give contact details for support

10 Documentation
The Clerk will maintain a Data Breach Register containing:
Description of the breach
Date discovered
Risk assessment
Decisions on notification
Actions taken
Lessons learned
This register must be retained in line with the Council's retention schedule.

11 Learning and Prevention
After each breach, the Council will:
Review what went wrong
Update policies or procedures
Provide additional training if needed
Improve technical or organisational controls
Patterns of repeated breaches will trigger a formal review.

12 Training and Awareness
All councillors, staff.

13. Approval
This policy was adopted by the Parish Council at its meeting on: 3.3.26

Signed: Chair of the Council Clerk / Responsible Officer