

**Billinge Chapel End Parish Council - Data Protection Policy**

**Table of Contents**
A. Purpose

B. Scope

C. Understanding and Identifying Personal Data Breaches
D. Reporting a Confirmed or Suspected Data Protection Breach
E. Incident Investigation
F. Reporting to the Information Commissioner’s Office (ICO)
G. Breach Register
H. Policy Evaluation and Review

**A. Purpose**

Billinge Chapel End Parish Council is committed to ensuring the protection of all personal data it processes. This policy outlines how the Council will respond to and manage data protection breaches, detailing the procedures for identifying, reporting, investigating, and mitigating the effects of a breach. The goal is to minimise harm to individuals and protect the reputation of the Council.

**B. Scope**

This policy applies to all personal data held by Billinge Chapel End Parish Council, regardless of whether it is in electronic or hard copy format. It includes data related to both staff and residents, as well as any other individuals with whom the Council interacts.

**C. Understanding and Identifying Personal Data Breaches**

A personal data breach occurs when there is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data. Breaches can be accidental or deliberate and may include but are not limited to the following:

* **Unauthorised disclosure** of personal data to third parties.
* **Sending information** to an incorrect recipient.
* **Phishing attacks** leading to the exposure of personal data or login credentials.
* **Loss or theft** of devices containing personal data (e.g., laptops, mobile devices).
* **Hacking** or other security breaches within Council systems.
* **Failure of equipment** resulting in the loss of personal data.

This policy applies to both confirmed breaches and suspected breaches that require investigation.

**D. Reporting a Confirmed or Suspected Data Protection Breach**

All staff, contractors, and volunteers must report any confirmed or suspected data protection breach immediately. This can be done by notifying the **Parish Clerk** directly. The Council recognises the importance of swift action to contain the breach and mitigate risks.

* **What to report**: Any unusual incidents involving personal data such as loss, theft, unauthorised access, or disclosure.
* **Who to notify**: Staff should report to the Parish Clerk, who will then notify the IT provider or other relevant authorities.
* **What to include**: Full details of the incident, including the nature of the breach, affected data, and any immediate steps taken.

**E. Incident Investigation**

Upon receiving a breach report, an investigation will be initiated. The investigation will determine the cause of the breach, the extent of the damage, and the appropriate actions to contain and remedy the breach.

* For IT-related breaches, the **IT Service Provider** will lead the investigation, ensuring technical issues are addressed.
* For non-IT incidents, the **Parish Clerk** will lead the investigation, involving relevant Council staff and external partners if necessary.

**Actions to take in response to a breach**:

* Immediately **contain** the breach and prevent further damage.
* Notify **affected individuals** where necessary.
* Record the breach, documenting all steps taken.
* Assess whether additional **staff training** or procedural changes are required.
* Review and improve **data security measures** where necessary.
* Evaluate whether disciplinary action is needed in case of negligence or breach of protocol.

**F. Reporting to the Information Commissioner’s Office (ICO)**

In line with the Data Protection Act 2018, the Council is required to notify the **Information Commissioner’s Office (ICO)** within 72 hours of becoming aware of a breach that may pose a risk to the rights and freedoms of individuals. The **Parish Clerk** will coordinate this process and ensure all relevant information is provided to the ICO.

* **Who will report**: The Parish Clerk will lead the reporting to the ICO, and other staff members may assist as required.
* **What will be reported**: A full description of the breach, the affected data, the steps taken to address the breach, and any recommendations for preventing future breaches.

**G. Breach Register**

All data protection breaches, whether confirmed or suspected, will be logged in the **Council’s Data Protection Breach Register**. The **Parish Clerk** will maintain this register, which will include details of the breach, its impact, the response actions taken, and any lessons learned. The register will be reviewed annually as part of the Council’s ongoing data protection practices.

**H. Policy Evaluation and Review**

This Data Protection Policy will be formally reviewed by the **Parish Clerk** at least once a year, or more frequently, if necessary, to ensure its relevance and compliance with current data protection laws. Additionally, the effectiveness of this policy and related procedures will be continuously monitored and evaluated.

Any changes to the policy will be approved by the **Parish Council** and communicated to all staff and relevant stakeholders.