

Data Breach Response Procedure

Hail Weston Parish Council

Purpose

Hail Weston Parish Council is committed to protecting personal data and complying with UK GDPR and the Data Protection Act 2018. This document explains the steps the Council will take in the event of a data breach (data leak).

What Is a Data Breach?

A data breach is any incident where personal data is:

- Lost, stolen, or accessed without permission
- Sent to the wrong person
- Altered without authorisation
- Disclosed accidentally or unlawfully

This applies to both electronic and paper records.

Immediate Response

As soon as a breach is suspected or identified, the Council will:

1. **Contain the breach**
 - Secure systems and accounts
 - Retrieve misdirected emails where possible
 - Recover lost documents
 - Restrict further unauthorised access
2. **Inform the Responsible Officer**
 - The Clerk (Data Protection Lead) will be notified immediately.

Assessment (Within 24 Hours)

The Clerk will assess:

- What data was involved
- How many individuals are affected
- Whether sensitive information was included
- The potential risk to individuals

All breaches will be recorded in the Council's Data Breach Register.

Reporting to the ICO

If the breach is likely to result in a risk to individuals' rights and freedoms, the Council will report it to the:

Information Commissioner's Office

- Notification will be made within **72 hours** of the Data Protection Lead being made aware.
- If reporting is not required, the reasoning will be documented.

Informing Affected Individuals

If there is a **high risk** to individuals, the Council will inform them without undue delay.

This communication will include:

- What happened
- What data was involved
- What actions the Council is taking
- Advice on protective steps
- Contact details for further information

Investigation and Remedial Action

The Council will:

- Investigate the cause of the breach
- Review procedures and safeguards
- Strengthen security measures where necessary
- Provide additional training if required

Lessons learned will be documented to prevent recurrence.

Prevention and Good Practice

To minimise risk, the Council:

- Restricts data access to authorised personnel
- Uses secure, password-protected systems
- Stores paper records securely
- Keeps software updated

- Provides data protection training

Approved by: Hail Weston Parish Council

Review Frequency: Annually or following any significant data breach