Willingale Parish Council

Data Breach Process and Policy

Adopted: 10th March 2026
Next Review: March 2028

Purpose

This policy outlines Willingale Parish Council's (Council) approach to identifying, managing, and reporting personal data breaches to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Scope

Applies to:

- All council employees, contractors, volunteers, and Councillors
- All personal data processed by or on behalf of the Council

Definition of a Data Breach

A personal data breach is a security incident that results in:

- Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

A special category data breach is a security incident that results in:

- Accidental or unlawful disclosure of highly sensitive personal information such as race, politics, religion, trade union membership, genetics, biometrics (for identification), health, sex life and sexual orientation

Examples include:

- Sending personal data to the wrong recipient
- Loss or theft of devices containing personal data
- Unauthorised access to Council systems

Roles and Responsibilities

Data Protection Officer (DPO) – the Clerk

- Lead breach investigations, assess risk, report to ICO if required Employees, contractors, volunteers, and elected members
- Immediately report suspected breaches to the DPO
- Support containment and recovery efforts
- Ensure resources and oversight for breach response

Reporting a Breach

All suspected breaches must be reported within 24 hours to the DPO via:

- Email: clerk@willingaleparishcouncil.org.uk

Use the Data Breach Reporting Form to provide details.

Breach Response Procedure

1. **Identification & Containment**

- Secure systems and prevent further data loss.

2. Assessment
- Determine nature, scope, and severity of breach.

3. Notification
- If risk to individuals is high, notify affected parties promptly.
- Report to ICO within 72 hours if required.

4. Recovery
- Restore data and systems.
- Implement corrective actions.

5. Review
- Conduct post-incident review.
- Update policies and training as needed.

Notification to the ICO

The DPO will assess whether the breach meets the threshold for reporting to the Information Commissioner's Office (ICO). If so, the report will include:
- Nature of the breach.
- Categories and number of individuals affected.
- Measures taken or proposed to address the breach.

Policy Review

This policy will be reviewed every two years or following a major breach incident.