

Slyne-with-Hest Parish Council

Data Protection Policy

Date Adopted : *October 2025*

Purpose

This Data Protection Policy outlines how **Slyne-with-Hest Parish Council** handles personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It applies to all individuals who collect, access, or use personal data on behalf of the Council.

Scope

This policy applies to all personal data processed by the Council, regardless of format (electronic, paper, verbal), and covers:

1. Residents' contact details
2. Employee records
3. Volunteer information
4. Service-related data
5. Any other personal data collected in the course of Council activities

Principles of Data Protection

The Council is committed to upholding the following principles:

Lawfulness, Fairness, and Transparency

1. Data will be processed lawfully and transparently.
2. Individuals will be informed about how their data is used via privacy notices.

Purpose Limitation

1. Data will only be collected for specified, legitimate purposes.
2. It will not be used for other purposes without further consent.

Data Minimisation

1. Only data necessary for the Council's functions will be collected.

Accuracy

1. Reasonable steps will be taken to ensure data is accurate and up to date.
2. A data audit will be conducted every two years.

Storage Limitation

1. Data will be retained only as long as necessary.
2. Retention schedules will be followed, and data will be securely deleted when no longer needed.

Integrity and Confidentiality

1. Appropriate security measures will be in place, including:
2. Password protection
3. Restricted access
4. Secure storage
5. Encryption where appropriate

Accountability

1. The Council will maintain records of processing activities.
2. Compliance will be monitored and reviewed regularly.

Roles and Responsibilities

Clerk (Data Protection Lead): Responsible for overseeing data protection compliance.

Councillors: Must follow this policy and report any concerns or breaches.

Employee(s): Must ensure data is handled securely and in line with this policy.

Data Subject Rights

Individuals have the right to:

1. Access their data
2. Request correction or deletion
3. Object to processing
4. Withdraw consent (where applicable)
5. Lodge complaints with the Information Commissioner's Office (ICO)

Requests should be directed to the Clerk via email to Clerk@slynewithhest-pc.gov.uk

Data Breaches

Any suspected data breach must be reported immediately to the Clerk. The Council will investigate and, *if necessary*, report the breach to the ICO within 72 hours.

Training and Awareness

All councillors and employees will receive basic data protection training via the National Cyber Security Centre (ncsc.gov.uk) and be made aware of this policy.

Definitions

Personal data: Any information relating to an identified or identifiable living individual.

Processing: Any operation performed on personal data, including collection, storage, use, and deletion.

Special categories of personal data: Includes data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

Criminal records data: Information about criminal convictions and offences.

Legal Basis for Processing

The Council will only process personal data where a lawful basis applies, including:

- Consent of the data subject
- Performance of a contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Special Category Data

Special category data will only be processed where a lawful condition applies, such as:

- Employment law obligations
- Vital interests
- Data made public by the individual
- Legal claims
- Substantial public interest
- Health or social care purposes
- Archiving, research, or statistical purposes

Subject Access Requests (SARs)

Individuals may request access to their personal data.

Requests should be submitted to the Clerk and may require proof of identity.

The Council will respond within one month, or notify if an extension is needed.

A fee may be charged for excessive or repeated requests.

Data Security Measures

The Council implements technical and organisational measures to protect data, including:

- Physical security (locked storage, secure disposal)

- IT security (passwords, encryption, access controls)
- Restrictions on remote access and personal devices
- Contracts with third party processors ensuring data protection compliance

International Data Transfers

The Council does not transfer personal data outside the European Economic Area (EEA).

Data Protection Impact Assessments (DPIAs)

DPIAs will be conducted for high risk processing activities, such as largescale data collection. This is unlikely to be necessary for Slyne with Hest parish council as very limited data is processed.

Individual Responsibilities

All councillors, employees, and volunteers must:

- Handle data securely and only for authorised purposes
- Report any data breaches or concerns
- Keep personal data up to date
- Follow Council policies and procedures

Disciplinary Consequences

Failure to comply with this policy may result in disciplinary action.

Serious breaches, such as unauthorised access or data destruction, may lead to dismissal.