

Hevingham Parish Council

Data Protection Policy

1. Introduction

This Policy sets out how the Parish Council ("the Council") collects, uses, stores, shares, and protects information and data. The Council is committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all other relevant legislation.

To conduct its business, services and duties, the Council processes a wide range of data. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

The Council will be as transparent as possible about its operations and will work closely with the public, local community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will make it freely available. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

The Council is a data controller and is responsible for ensuring that personal data is processed lawfully, fairly, and transparently.

The Clerk is responsible for overseeing data protection and advising the Council on compliance.

2. Purpose of the Policy

The purpose of this policy is to:

- Protect the rights and privacy of individuals whose data is held by the Council.
- Ensure compliance with data protection law.
- Establish clear responsibilities for councillors, employees, volunteers, and contractors.
- Provide transparency on how personal data is handled.

3. Scope

This policy applies to:

- All Councillors and employees of the Council.
- Any volunteers, contractors, or third parties working on behalf of the Council.
- All personal data that the Council processes in any format, including electronic, paper, audio, and visual records.

4. Terminology

Data subject – means the person whose personal data is being processed.

Personal data – means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person. Examples include: a name, a photo, an address, date of birth, an email address and bank details.

Sensitive personal data – includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data is to be processed.

Data processor – in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data – means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- aligning, combining, blocking, erasing or destroying the information or data, regardless of the technology used.

5. Processing Personal Data

The Council collects and uses personal data for purposes including:

- Managing Council meetings, public consultations, and statutory notices
- Responding to enquiries from residents
- Administering finances, grants, contracts, and assets
- Maintaining employment and personnel records
- Operating CCTV, websites, and mailing lists
- Assisting regulatory and law enforcement agencies.
- Undertaking surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with the Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however wherever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Council can keep their personal data accurate and up to date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided

6. Data Protection Principles

The Council will ensure that personal data is:

1. Processed lawfully, fairly, and transparently

All data processed will be done in accordance with a lawful basis, see section 6. Data subjects will be informed about why their data is being processed, who it will be shared with and how long it will be retained by use of a Privacy Statement or Privacy Notice.

2. Collected for specific, explicit, and legitimate purposes

Personal Data will only be used for the purpose/s it was collected for.

3. Adequate, relevant, and limited to what is necessary

The collection and processing of Personal Data will be limited to that which is necessary.

4. Accurate and kept up to date

The Council recognises the requirements to keep Personal Data up to date.

5. Kept only for as long as necessary

In line with the Council's Records Management Policy

6. Processed securely

In line with this policy and the Council's IT Policy

7. Lawful Bases for Processing

The Council will process personal data only where at least one lawful basis applies, including:

- The individual has **consented** to the processing.
- Processing is necessary for the performance of a **contract** or agreement with the individual.
- Processing is required under a **legal obligation**.
- Processing is necessary to protect the **vital interests** of the individual.
- Processing is necessary to carry out **public functions**.
- Processing is necessary to pursue the **legitimate interests** of the data controller or third parties.

Attention is paid to the processing of any sensitive personal information, and the Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual.
- Required by law to process the data for employment purposes.
- A requirement to protect the vital interests of the individual or another person.

8. Rights of Individuals

Individuals have the following rights regarding their personal data:

- **Right to be informed**
- **Right of access** (Subject Access Request)
- **Right to rectification**
- **Right to erasure** (where applicable)
- **Right to restrict processing**
- **Right to data portability**
- **Right to object**
- **Rights in relation to automated decision-making**

The Clerk will be responsible for responding to all requests, any requests received by staff or Councillors should be forwarded to the Clerk. Requests will be responded to within **one month** unless an extension is permitted by law.

Individuals have the right to make a complaint in line with the Council's Complaints Policy or directly to the Information Commissioners Office (ICO) casework@ico.org.uk 0303 123 1113.

9. Data Sharing

The Council may share personal data with:

- Government bodies (e.g., HMRC, ICO)
- Service providers or contractors acting on behalf of the Council
- Law enforcement agencies (where legally required)

Data will never be sold to third parties.

Data sharing agreements will be in place where appropriate.

10. Data Retention

Personal data will be kept only for as long as necessary. A separate Retention List sets out specific retention periods.

11. Data Security

The Council will implement appropriate technical and organisational measures to protect data, including:

- Secure email and password protection
- Locked filing cabinets for paper records
- Restricted access to systems and data
- Regular backups

- Encryption where appropriate
- Secure disposal of data

Councillors and staff must ensure personal devices used for Council work are password-protected.

12. Data Breaches

A data breach includes loss, theft, unauthorised access, disclosure, or destruction of personal data. All breaches must be reported to the Clerk immediately. Where a breach poses a risk to individuals, the Council will notify the ICO within 72 hours and inform affected individuals as required.

A record will be kept of all data breaches to include details of the breach, action that was taken at the time and action agreed to mitigate against future breaches.

13. Training and Awareness

Councillors, employees, and volunteers will receive appropriate training on:

- Data protection responsibilities
- Secure data handling
- Recognising and reporting data breaches

14. Review of Policy

This policy will be reviewed every 2 years or sooner if legislation or operational processes change.

Adopted July 2026

For review July 2028