HEDLEYHOPE PARISH COUNCIL

Data Protection Policy

1) Purpose

This policy outlines how Hedleyhope Parish Council (the Council) collects, uses, and protects personal information to comply with its legal obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2) Scope

This policy applies to all councillors and employees of the Council when handling personal data and who must comply with its terms. It covers:

- the processing of all personal information whose use is controlled by the Council;
- all personal information handled, stored, processed or shared by the Council whether organised and stored in physical or IT-based record systems.

The Council's own related policies are listed below:

- Document Retention Policy
- Privacy Policy
- Freedom of Information Policy

3) Data Protection Principles

The Council adheres to the following key principles of data protection:

1. *Lawfulness, Fairness and Transparency*: personal data will be processed lawfully, fairly and in a transparent manner.
2. *Purpose Limitation*: data is collected for specified, explicit, and legitimate purposes.
3. *Data Minimisation*: data collected will be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
4. *Accuracy*: data will be accurate and, where necessary, kept up-to-date.
5. *Storage Limitation*: data will be retained only for as long as necessary.
6. *Integrity and Confidentiality*: data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.
7. *Accountability*: the Council is responsible for compliance with these principles.

4) Roles and Responsibilities

Parish Council

- The Council is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required. The Council will be

responsible for ensuring that it complies with its responsibilities under the data protection legislation.
- Approves and reviews this policy regularly.
- Ensures appropriate oversight of data protection activities.

Parish Clerk

- Acts as the Data Protection Lead for the Council.
- Maintains records of data processing activities.
- Responds to data subject rights requests (e.g. access, rectification).
- Reports data breaches to the ICO and affected individuals when necessary.

Councillors

- Are responsible for understanding their data protection duties.
- Must handle all personal data in line with this policy.
- Must not disclose personal data without lawful authority.
- Must report any data breaches or concerns promptly to the Clerk.

Staff, Contractors, and Volunteers

- Must follow this policy.
- Report any data breaches, risks, or concerns promptly to the Clerk.

5) Collection and Use of Personal Data

The Council collects and uses personal data only where necessary to fulfil its official duties and functions. Individuals are informed of the purpose of data collection, as well as their rights under UK data protection laws.

Lawful Bases for Data Processing

Personal data is processed by the Council under one of the six lawful bases outlined below:

1. *Consent* – individuals have provided clear, freely-given and unambiguous permission for their data to be used for a specific purpose. They retain the right to withdraw their consent at any time.
2. *Contract* - processing that is necessary to enter into or perform a contract, e.g. employment contracts or agreements with contractors.
3. *Legal Obligation* – to comply with legal requirements, excluding contractual obligations, e.g. financial reporting, responding to Freedom of Information or Subject Access Requests, and keeping accounting records.
4. *Vital Interests* – data may be processed where it is necessary to protect someone's life in an emergency, e.g. a medical incident at a Council-organised event.
5. *Public Task* – applies when processing is required for tasks carried out in the public interest or fulfilling statutory duties and is the most frequently used lawful basis by Parish Councils.

6. *Legitimate Interests* – processing is necessary for the legitimate interests of the Council or a third party, provided these are not overridden by the rights and freedoms of the individual. This basis is used rarely by Parish Councils and is not applicable when performing official public functions.

Types of Data Collected

The Council may collect various types of personal data, including:

- Contact details (names, addresses, phone numbers, and email addresses).
- Planning application feedback.
- Financial and contractual information (invoices, payroll, expenses).
- Correspondence from residents, community groups, or other authorities.
- Details of suppliers, contractors, and service providers.
- Volunteer, employee, or councillor contact and emergency details.

Purposes for Data Collection

Personal data is collected for the following purposes:

- Responding to resident enquiries and facilitating community engagement.
- Managing finances, grants, contracts, and procurement processes.
- Handling planning consultations and collecting feedback.
- Maintaining minutes, attendance records, and other registers.
- Organising public consultations and events.
- Managing employment and volunteer roles.
- Publishing councillor contact details and declarations of interest, as legally required.

Ensuring Proper Use of Data

The Council is committed to using personal data responsibly:

- Only data that is necessary and relevant for the task is collected.
- Data is used exclusively for the purpose for which it was obtained, unless a legal requirement or another compatible purpose arises.
- Information is shared only with authorised individuals or organisations and only when a lawful basis exists.
- Data is regularly reviewed to determine if it is still required and is securely disposed of when no longer needed.
- Councillors and staff are made aware of the importance of proper data collection and usage in line with this policy.

Data Held About Council Staff, Councillors, and Volunteers

The Council holds personal data relating to staff and councillors. Such information is used to comply with legal obligations in relation to employment and administrative obligations, and may be shared with other regulatory authorities when appropriate. Personal data may also be used when providing references.

The Council may also hold personal information about other individuals who engage with the Council, such as volunteers and guests. This information is managed in line with data protection principles and is not kept longer than is necessary.

6) Data Sharing and Disclosure

The Council is committed to protecting the confidentiality and security of personal data. Personal data will only be shared with third parties under the following circumstances:

- There is a lawful basis for doing so, in accordance with UK GDPR requirements.
- It is necessary to fulfil a statutory function or public task.
- The data subject has provided informed consent, where required.
- There is a legal obligation to disclose the data (such as to HMRC or the police).
- It is necessary to protect an individual's vital interests (for example, in a medical emergency).

Personal data is never sold or passed to third parties for marketing purposes.

The Council may share personal data with the following entities:

- Local government bodies, such as the county council, where collaboration is required (e.g. on planning or highways matters).
- Regulatory authorities, such as the Information Commissioner's Office (ICO) or the Local Government Ombudsman, when legally required or requested.
- Service providers and contractors, including payroll providers, auditors, or IT support, where access to personal data is necessary to deliver a contracted service.
- Emergency services, in situations where data is needed to protect life or safety.
- Councillors, for carrying out official council duties, provided they are acting under the Council's authority and within the scope of their role.

Third-Party Contracts and Data Processors

When engaging third-party processors, such as cloud storage providers, the Council will ensure:

- A written contract is in place that meets UK GDPR requirements.
- The third party is fully compliant with data protection laws.
- Data is processed solely for the purposes specified in the contract.
- The third party implements suitable security measures.
- All processors agree to handle data only under the Council's instructions and not to use the data for their own purposes.

Sharing Data with Consent

Where personal data is shared based on consent, the Council will:

- Clearly explain what data will be shared, with whom, and for what purpose.
- Obtain freely given, specific, informed, and unambiguous consent.
- Keep a record of the consent, including when and how it was given.
- Allow individuals to withdraw consent at any time and act on such requests promptly.

Disclosures Required by Law

In certain circumstances, the Council is legally required to disclose personal data. Such circumstances include:

- Responding to a court order.
- For the prevention or detection of crime, on request by the police.
- To obtain legal advice or for legal proceedings.
- Meeting legal reporting requirements, such as those under the Local Government Transparency Code.

In all such cases, the Council will verify the legitimacy of the legal request and disclose only the minimum amount of personal data necessary.

Data-Sharing Safeguards

To ensure data sharing is secure and appropriate, the Council will:

- Assess all disclosures for risk and necessity before proceeding.
- Use secure methods for sharing data, such as encrypted email or registered post.
- Limit access to shared data to authorised recipients only.
- Log any significant or high-risk data sharing, and conduct a Data Protection Impact Assessment (DPIA) when necessary.

7) Data Subject Rights

Under the UK GDPR, individuals - referred to as data subjects - are granted a number of specific rights regarding their personal data. The Council recognises the importance of these rights and ensures that individuals whose data it holds are able to exercise them as outlined below.

- The right to be informed about the collection and use of personal data.
- The right of access to personal data.
- The right to rectification of inaccurate or incomplete data.
- The right to erasure (the ‘right to be forgotten’), subject to legal requirements.
- The right to restrict or object to processing of data.
- The right to data portability (where applicable).
- The right to lodge a complaint with the Information Commissioner's Office (ICO).

Further details can be found in the Council’s Privacy Policy.

8) Data Security

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

Physical Security

- Paper records containing personal data are stored in locked cabinets.
- Access to physical records is restricted.
- The Council's storage locations are kept secure.
- Confidential information is not left unattended in public or shared areas.

Electronic Security

- All computers and devices used for Council business are password-protected and, where possible, encrypted. Passwords are regularly changed.
- Antivirus software, firewalls, and security patches are regularly updated.
- Councillors and staff use secure email systems for any communications involving personal data.
- Access to personal data held electronically is restricted through role-based access controls or permissions.
- Regular backups of digital data are performed and stored securely, with test recoveries conducted periodically.
- Data is never saved onto unprotected mobile devices such as tablets or smartphones.

Disposal of Data

- Paper documents containing personal data are disposed of securely.
- Electronic data is securely deleted when no longer required, ensuring that deleted files cannot be recovered.
- Equipment that is no longer in use is wiped clean of all data before disposal, in line with best practices.

Security Monitoring and Audits

- The Council will periodically review its data security practices and perform internal checks or audits to ensure continued compliance.
- Any weaknesses identified will be addressed promptly.

9) Data Breaches

A personal data breach under the UK GDPR is defined as a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Such breaches can occur in a variety of ways, including but not limited to:

- Access to personal data by an unauthorised third party.
- Deliberate or accidental action (or inaction) by the controller or processor.
- Sending personal data to the incorrect recipient.

- Loss or theft of devices containing personal data.
- Unauthorised alteration or loss of availability of personal data.
- Deliberate attacks on IT systems, such as phishing or malware.

Immediate Actions in the Event of a Suspected or Actual Data Breach

If any councillor, staff member, or volunteer discovers, or suspects, a data breach, the following steps should be taken:

1. Report the breach immediately to the Clerk.
2. Do not attempt to conceal or resolve the breach.
3. Preserve all evidence related to the breach, including emails, documents, and devices.
4. Take reasonable steps to mitigate further damage, such as recalling emails, locking devices, or securing files, where possible.

If a third-party data processor becomes aware of a breach, they must notify the Council without delay. The Council (as data controller) is responsible for assessing the breach and reporting to the Information Commissioner's Office (ICO) if necessary.

Assessment and Notification Procedures

On notification of a potential or actual breach, the Clerk will conduct an assessment to determine the nature and seriousness of the incident. This includes evaluating:

- The types and sensitivity (e.g. financial or contact details) of data involved.
- The number of people affected.
- The potential consequences and risks for individuals.
- The security measures in place to protect the data.
- Any immediate actions that can be taken to reduce risks to individuals.

Reporting to the ICO

If there is likely to pose a risk to individuals, the breach must be reported to the Information Commissioner's Office (ICO) via the ICO website https://ico.org.uk/for-organisations/report-a-breach/ within 72 hours of becoming aware of the breach, where feasible. The report should include:

- A description of the nature of the breach, including the categories and approximate number of data subjects and personal data records involved.
- The name and contact details for further enquiries.
- An outline of the likely consequences of the breach.
- The measures taken or proposed to address the breach and mitigate its possible adverse effects.

Notification of Data Subjects

If the breach is likely to result in a high risk to affected individuals, the Clerk must inform them without undue delay, unless the data would be unintelligible to

unauthorised persons or measures have already been taken to mitigate any risks. The notification should include a description of the breach, who to contact with questions or concerns and the measures taken to address and mitigate the risks.

Investigation and Record-Keeping

The Clerk will initiate an investigation into the breach to include establishing how the breach occurred, whether it could have been prevented, and reviewing current procedures. The Council will consider recommendations for corrective action and decide on their implementation.

All data breaches must be documented, regardless of whether they are reported to individuals. These records should be used to improve the security of personal data and prevent future incidents.

10) Retention and Disposal

Personal data will be retained only as long as necessary for the purposes for which it was collected and in accordance with the council's retention schedule. Data will be securely destroyed or deleted when no longer required. Further information can be found in the Council's Document Retention Policy.

11) Policy Review

This policy will be reviewed annually, or sooner if there are significant changes to legislation or Council procedures.

12) Contact

For further information, to exercise your rights, or to report a concern, please contact the Parish Clerk at hedleyhopeparishcouncil@gmail.com