Heighington Parish Council

Data Protection Policy

Document Ref:	POL/DP
Status:	Approved
Version:	3.0
Date of approval:	11 May 2026
Minute reference:	015/M/26
Date of next review:	May 2028 (or if legislation changes)

Version Control:

Version: 3.0
Amended by: Clerk
Details of amendments: Review at Annual Parish Council meeting. Formatting corrections.
Date approved: 11/05/2026
Minute reference: 015/M/26

Version: 2.0
Amended by: Clerk
Details of amendments: Review at Annual Parish Council meeting. Reformatting.
Date approved: 13/05/2024
Minute reference: 014/M/24

Version: 1.0
Amended by: Clerk
Details of amendments: First version
Date approved: 14/03/2022
Minute reference: 184/M/21

1. Purpose

1.1 The purpose of this policy is to ensure that employees, councillors and volunteers handling personal information at Heighington Parish Council (the 'Council') are fully aware of the requirements of the General Data Protection Regulations (GDPR) and comply with data protection procedures. The policy also aims to ensure that data subjects are aware of their rights.

1.2 The aim of this policy is to outline how the Council meets its legal obligations in safeguarding confidentiality and adheres to information security standards.

2 Scope

2.1 This policy applies to all councillors, employees and volunteers of the Council and will be referred to as role holders within this policy.

2.2 This Data Protection Policy 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.

3 Policy statement

3.1 The Council recognises its responsibility to comply with the GDPR 2018 which regulates the use of personal data.

3.2 Role holders have a duty to comply with the policy when handling personal data.

4 Definitions

4.1 A list of definitions of the technical terms used in this policy is below:

- Data Controller
  The person(s) who, on behalf of the Council, decides what personal information the Council will hold and how long it will be held or used.
- Data Protection Officer
  The person(s) responsible for ensuring that the Council follows data protection policy and complies with the relevant legislation.
- Information Commissioner's Office (ICO)
  A UK independent body responsible for upholding the information rights of the public.
- Personal Information
  Information about living individuals that enables them to be identified. E.g. names and addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers, employees or members of the public.
- Sensitive data
  Includes but is not limited to data relating to racial or ethnic origin, political opinions,

religious or similar beliefs, trade union membership, physical or mental health, criminal record or proceedings.

The Data Protection Policy

The Council recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

General Data Protection Regulations (GDPR)

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper. The Council has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, Council staff and members must ensure that:

- **Data is processed fairly, lawfully and in a transparent manner**
  This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.

- **Data is processed for specified purposes only**
  This means that data is collected for specific, explicit and legitimate purposes only.

- **Data is relevant to what it is needed for**
  Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

- **Data is accurate and kept up to date and is not kept longer than it is needed**
  Personal data should be accurate, if it is not, it should be corrected. Data no longer needed will be shredded or securely disposed of.

- **Data is processed in accordance with the rights of individuals**
  Individuals must be informed, upon request, of all the personal information held about them.

- **Data is kept securely**
  There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Storing and accessing data

The Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.

The Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the Council Office and are not available for public access. All data stored on the Council Office computers are password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of Council's document retention policy, it will be shredded or securely deleted from the computer.

The Council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy, email or social media). If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed
- The period the Council intends to process it for
- Anyone who has access to the personal data

The response must be sent within 30 days and should be free of charge.

If a SAR includes personal data of other individuals, the Council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

Please see "Subject Access Request Procedure" for more details.

Confidentiality

Council members and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.