Hatherton and Walgherton Parish Council

Data protection policy

Introduction

Hatherton and Walgherton Parish Council (HWPC) needs to gather and use certain personal information about individuals.

These individuals can include Parish Clerk of HWPC, residents of Hatherton and Walgherton and other people the council has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Council's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures HWPC:

- Complies with data protection law and follows good practice
- Protects the rights of Councillors, residents and others
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 and UK General Data Protection Regulation describe how organisations — including HWPC — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to:

- The Parish Clerk
- The Councillors of the Parish Council
- Contractors, suppliers and other people working on behalf of HWPC

It applies to all data that the Council holds relating to identifiable individuals, even if that information technically falls outside of the Regulations. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to identifiable individuals

Lawful basis for processing personal data

The Council processes data for the following reasons:

- To maintain records of Councillors including: maintaining an up-to-date list of Councillors for the Council and residents to see; enabling communication with Councillors by post, email or telephone; enabling communication with residents.
- To retain a list of residents interested in receiving local news.

Data protection risks

This policy helps to protect the Council from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all residents should be free to choose how the Council uses data relating to them.
- **Reputational damage.** For instance, the Council could suffer if hackers successfully gained access to sensitive data.

Responsibilities

The Clerk of the Parish Council has responsibility for ensuring data is collected, stored and handled appropriately.

Each person who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Councillors** collectively are ultimately responsible for ensuring that the Council meets its legal obligations.
- The **Parish Clerk** is responsible for:
    - Keeping the Councillors updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.

- Handling data protection questions from councillors and anyone else covered by this policy.
- Dealing with requests from individuals to see the data that the Council holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the Council's sensitive data.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets e.g. newspapers.

- The **Parish Clerk and Webmaster(s)** are responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the Council is considering using to store or process data. For instance, cloud computing services.

General guidelines for Councillors

- The only people able to access data covered by this policy should be those who **need it for their responsibility within the Council**. This would include, for example, contacting other councillors and emailing newsletters.
- Data **should not be shared informally**. When access to confidential information is required, Councillors can request it from the Parish Clerk.
- **The Council will provide training** to all Councillors to help them understand their responsibilities when handling data.
- Councillors should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Council or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Councillors **should request help** from the Parish Clerk if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely on paper can be directed to the Parish Clerk.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When data is stored on paper such as councillor applications:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Councillors should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
  - Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
  - If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
  - Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
  - Data should be **backed up frequently**. Those backups should be tested regularly, in line with the Council's standard backup procedures.
  - Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones without adequate password protection and/or encryption.
  - All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, misuse or theft:

- When working with personal data in a public place, Councillors should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure. The Parish Clerk can show Councillors how to transfer data securely.
- Data must be **encrypted before being transferred electronically**. The Parish Clerk can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.

Data accuracy

The law requires the Council to take reasonable steps to ensure data is kept accurate and up to date. It is most important that the personal data is accurate, and greater effort should be put into ensuring its accuracy. It is the responsibility of all Councillors who use personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Councillors and the Council should not create any unnecessary additional data sets.
- The Council should **take every opportunity to ensure data is updated.** For instance, by confirming a resident's details annually.

- Data should be **updated as inaccuracies are discovered**. For instance, if a resident can no longer be reached on their stored email address, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by the HWPC are entitled to:

- Ask **what information** the Council holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the Council is meeting its data protection obligations.

If an individual contacts the Council requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the Parish Clerk at **parish.clerk@handw-pc.gov.uk**. The Parish Clerk can supply a standard request form, although individuals do not have to use this. Individuals will not be charged for a subject access request. The Parish Clerk will aim to provide the relevant data within 14 days. The Parish Clerk will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act/GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Council will disclose requested data. However, the Parish Clerk will ensure the request is legitimate, seeking assistance from the Councillors and from the Council's legal advisers where necessary.

Providing information

The Council aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the Council has a privacy statement, setting out how data relating to individuals is used by the Council.

This is available on request. A version of this statement is also available on the Council's website.

Adopted: 23/7/2018
Reviewed: March 2025
Next Review: March 2026