Hassocks Parish Council
Data Protection Policy
Approved 10 February 2025 (PC25/131.3)

DATA PROTECTION POLICY

1. Introduction

Data protection is about respecting people's right to privacy. It ensures that individuals' personal data is handled with care, fairness, and transparency. Good data protection is based on the legal principles that guide policy and practice.

2. Legal Context

The Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) adopted in 2021, govern the protection of personal data and privacy rights. The Data (Use and Access) Act (DUAA) became law in June 2025; it amends and supplements the existing data protection legislation.

These documents establish a comprehensive legal framework that controls how personal information is used by organizations, including businesses, councils and government departments.

The law is based on seven key principles:

- **Lawfulness, fairness and transparency** - data must be processed legally, fairly, and in a way that is clear to individuals.

- **Purpose limitation** - data should only be collected for specific, legitimate purposes and not used for anything incompatible with those purposes.

- **Data mimimisation** - collect only the necessary data for the stated purpose and no more than needed.

- **Accuracy** - ensure data is correct and updated as necessary; inaccurate data should be corrected or deleted.

- **Storage limitation** - retain data only for as long as it is needed for the purpose; then securely delete or anonymise it.

- **Integrity and confidentiality** - protect data against unauthorised access, loss, or damage using appropriate security measures.

- **Accountability** – organisations must not only comply but also demonstrate compliance (e.g., policies, records, audits).

Under UK GDPR Article 6(1), data processing is only lawful if at least one of the following applies:

(a) Consent - the data subject has given consent to the processing of his or her personal data for one or more specific purposes

(b) Contract - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

(c) Legal obligation - processing is necessary for compliance with a legal obligation to which the controller is subject

(d) Vital interests – the processing is necessary to protect someone's life

(e) Public task - processing is necessary for a task carried out in the public interest, or in the exercise of official authority given to the council, but there is no legal requirement to do it i.e. answering general correspondence

(f) Legitimate interests - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, i.e. CCTV on buildings

3. Responsibilities

3.1. Hassocks Parish Council is a data controller with responsibility for UK GDPR compliance and must ensure:

- a lawful basis for processing personal data.
- transparency (privacy notices)
- data subject rights are respected
- appropriate security measures are in place

3.2. The Clerk is responsible for day-to-day oversight and will advise Councillors and staff on good practice to ensure personal data is managed lawfully, securely, and effectively.

3.3. As required by law, the Council is registered as a Data Controller with the Information Commissioner's Office (Ref: ZA356087).

3.4. Hassocks Parish Council has adopted and published a Privacy Notice which provides information about how personal data is collected, used and protected. It outlines the lawful basis for processing personal data and informs individuals of their rights under GDPR.

4. Access to information

4.1. Any employees, Councillors, residents, customers and other data subjects have a right to:

- ask what personal information the Council holds
- ask what this information is used for
- be provided with a copy of the information
- be given details of the purposes for which the council uses the information and any other person's organisations to whom it is disclosed

4.2. If it is felt by the data subject that any personal information held is incorrect the individual may request that it be amended. The council must advise the individual within 21 days whether or not the amendment has been made.

5. Storage and retention

5.1. Hassocks Parish Council uses a combination of physical, electronic, and managerial measures to safeguard personal information.

- Physical Measures – secure storage such as locked filing cabinets and restricted access to council offices.
- Electronic Measures – password-protected systems, encryption, firewalls, and regular software updates to prevent unauthorised access.
- Managerial Measures – policies and procedures for handling data, staff training on data protection and regular compliance reviews.

5.2. The Council will keep different types of information for differing lengths of time, depending on legal and operational requirements. More information can be found in the Council's Document Retention Scheme.

6. Data breaches

6.1. All suspected or actual data breaches must be reported to the Clerk immediately.

6.2. The Clerk will

- Record the breach in the Data Breach Log

- Assess the level of risk to individuals
- Report notifiable breaches to the ICO within 72 hours where necessary
- Notify affected individuals if there is a high risk to their rights or freedoms

7. Data Protection Terminology

7.1. **PERSONAL DATA** means any information that can identify a living person directly or indirectly (e.g. email, job title, address, reference number). It applies to records in any format, including digital files, paper documents, audio and video.

7.2. A **DATA SUBJECT** is any identifiable living individual (natural person) whose personal data is being collected, processed, or stored. For example:

- If the Council collects names and addresses for a mailing list, these people are the data subjects.
- As an employer the Council stores employee records, the employees are the data subjects.

Under UK GDPR laws, a data subject has specific rights regarding their personal data, such as:

- **Right of access** – to know what data is held about them
- **Right to rectification** – to correct inaccurate data.
- **Right to erasure** – to request deletion of their data.
- **Right to restrict processing** – to limit how their data is used.
- **Right to data portability** – to receive their data in a usable format.
- **Right to object** – to stop certain types of processing.
- **Right to be informed** - to know how the Council collects, uses and shares personal data.
- **Rights related to automated decision-making and profiling**

7.3. A **DATA CONTROLLER** is the person, organization, or entity that determines the purposes and means of processing personal data. In other words, they decide:

- Why the data is being processed (the purpose).
- How the data will be processed (the method).

Data controllers must register with the Information Commissioner's Office (ICO).

7.4. **DATA PROCESSING** means obtaining, recording or holding information or carrying out any operation on the information or data, including the following examples:

- **Collecting Data** - receiving contact details via a website form or taking photographs at an event
- **Recording Data** - entering resident details into a spreadsheet or database or writing down meeting attendees in a logbook
- **Organising or Structuring Data** - sorting a mailing list by postcode or creating folders for different types of correspondence
- **Storing Data** - keeping paper or digital files or saving emails in an inbox, archive or server
- **Using Data** - sending newsletters to residents using their email addresses

or using phone numbers to confirm appointments
- **Retrieving Data** - searching a directory for a resident's previous complaint or looking up archived meeting notes
- **Disclosing Data** - sharing contact details with a contractor for maintenance work or providing information to auditors or regulators
- **Erasing or Destroying Data** - shredding old paper records or deleting outdated files from the server

Essentially, if you do anything with personal data, it counts as processing.

7.5. Controllers can appoint a **DATA PROCESSOR** (third parties who process data on their behalf), but the controller remains accountable.

7.6. A **DATA PROTECTION OFFICER** is an independent expert appointed to oversee compliance with data protection laws.

7.7. A **DATA BREACH** is an incident where personal data is accessed, disclosed, or stolen by an unauthorized person or system - whether by accident or on purpose. Common types of data breach include personal and financial information which can lead to identity theft, financial loss, reputational damage and legal consequences.

7.8. **SPECIAL CATEGORY DATA** is a type of personal data that is more sensitive and needs extra protection. It includes personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health, sex life and sexual orientation.