



Key principles

Hive collects and uses certain types of information to carry out its work. This personal information must be collected and dealt with appropriately, whether digitally, on paper, or on other material.

Data protection laws describe how organisations must collect, handle and store all personal data. Ensuring and demonstrating compliance is underpinned by the following principles.

Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data definitions

- **Personal information**

Information about living individuals that enables them to be identified (eg. name and address). It does not apply to information about organisations, companies and agencies, but applies to named persons, such as individual volunteers or employees.

- **Special category data**

Information about racial or ethnic origin, political opinions, religious or similar beliefs, health (mental or physical), sexual life, trade union membership and criminal convictions (see below). This data is subject to greater restrictions than other data.

- **Criminal Offence Data**

Information concerning criminal allegations, proceedings or convictions. This is subject to greater restrictions than special category data and should not be processed without official authority.

- **Data Controller**

Hive is a Data Controller, which means that it determines what purposes personal information will be used for. As a not-for-profit organisation which processes data only to serve the needs of its users, Hive is exempt from registration with the Information Commissioner's Office (ICO).



Data Protection Officer

Hive will appoint a Data Protection Officer, responsible for ensuring that it follows its data protection policy and complies with the GDPR and related legislation (see appendix 1).

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Individual Rights

Hive will uphold the rights of data subjects to access and retain control over their personal data, through the:

- **Right to be Informed**
by ensuring they are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights and how to exercise them.
- **Right to Access**
by ensuring that they are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- **Right to Rectification**
by correcting personal data that is found to be inaccurate. We will advise them how to let us know that their data is inaccurate, and it will be rectified without undue delay.
- **Right to Erasure ('the right to be forgotten')**
by advising them of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Right to Restrict Processing**
by restricting processing when a valid request is received from them, and informing them of how to exercise this right.
- **Right to Data Portability**
by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.
- **Right to Object**
by stopping processing personal data, unless legitimate grounds for the processing can be demonstrated which override their interest, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

Legislation

This policy aims to enact and the rights and rules in the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018 (DPA2018), as amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Privacy and Electronic Communications Regulations (PECR).



Data Processing

Collection and consent

Informed consent is when a Data Subject clearly understands:

- why their information is needed
- who it will be shared with
- the possible consequences of them agreeing or refusing the proposed use of the data

and then gives their consent.

Hive will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Hive will ensure that the Data Subject:

- clearly understands why the information is needed
- understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing.
- as far as reasonably possible, grants explicit consent, either written or verbal, for data to be processed.
- is, as far as reasonably practicable, competent to give consent and has given so freely without any duress.
- has received sufficient information on why their data is needed and how it will be used.

Processing and storage

Hive intends to ensure that personal information is treated lawfully and correctly. To that end, Hive will adhere to the principles of data protection, as detailed in the GDPR. Specifically, the principles require that personal information:

- shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- shall be obtained only for one or more of the purposes specified in the regulations, and shall not be processed in any manner incompatible with that purpose or those purposes.
- shall be adequate, relevant and not excessive in relation to those purposes.
- shall be accurate and, where necessary, kept up to date.
- shall not be kept for longer than is necessary, and will then be disposed of appropriately (including ensuring that any data is non-recoverable from IT assets which are disposed of).
- shall only be available to authorised staff and volunteers.
- shall be processed in accordance with the rights of data subjects under the regulations.
- shall be stored securely with appropriate technical and other measures to safeguard personal information and to prevent unauthorised or unlawful processing, or accidental loss or destruction of, or damage to, personal information.
- shall not be transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.



Hive will, through appropriate management, strict application of criteria and controls:

- observe fully conditions regarding the fair collection and processing of information.
- meet its legal obligations to specify the purposes for which information is used.
- collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
- ensure the quality of information used.
- ensure that the rights of people about whom information is held can be fully exercised (above).
- respond promptly and courteously to any requests from individuals to exercise their rights in regard to their personal data, or any questions about the processing of personal information.
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- set out clearly how it handles personal information.
- set out clear procedures for responding to requests for information.

In addition, Hive will ensure that everyone processing personal information:

- understands that they are responsible for following good data protection practice
- is appropriately trained to do so
- is appropriately supervised
- knows where to address questions about the processing of data
- understands that a breach of this policy may lead to disciplinary action being taken against them.

Data Sharing and Disclosure

Any third-party requests for data must be referred to the Data Protection Officer who will assess the validity of the request before complying.

Hive shares data with other agencies such as the local authority, funding bodies and other voluntary agencies. Data will be anonymised or supplied only as statistical aggregates for these purposes.

The law allows Hive to disclose personal data (including sensitive data) without the data subject's consent when:

- carrying out a legal duty
- protecting vital interests of a Data Subject
- the Data Subject has already made the information public
- conducting any legal proceedings, obtaining legal advice or defending any legal rights.
- monitoring for equal opportunities purposes (eg. race, disability or religion)
- providing a confidential service where the Data Subject's consent cannot be obtained, or where it is reasonable to proceed without consent (eg. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures).

Review

Hive will regularly review and audit the ways it collects and processes personal information, and assess and evaluate its methods and performances in relation to handling data.

This policy will be reviewed annually, or sooner if necessary, to reflect best practice in data processing and security, and to ensure compliance with any changes or amendments to the relevant legislation.



Appendix 1: Data Protection Officer

The Data Protection Officer is:

Joy Hart (Manager)	joy.hart@hivebradford.org.uk	01274 598928
---------------------------	------------------------------	--------------

Appendix 2: Retention of Records

Organisation and Membership	
Memorandum and Articles of Association and variations	Permanently
Certificate of incorporation, Charity registration	Permanently
Trustee and General Meeting minutes	Permanently
Trustees' Annual Reports and Accounts	6 years from the date of signing
Employer's liability certificate	40 years
Insurance policies	Permanently
Building records (including planning consent, building control, surveys, inspections and legal documents)	Permanently
Asset register	Permanently
Statutory Registers (eg. members, Trustees, persons with significant control, conflicts of interest)	Permanently
Membership records	10 years
Financial records	
Invoices and receipts, payroll, pension and tax	6 years from the end of the financial year
Leases	12 years after end of lease
Rental or Hire Purchase agreements	6 years after end of agreement
Title deeds	Permanently
Health and Safety	
Health & Safety records (including records relating to an injury or accident at work, risk assessments, accident books)	12 years following the date of the record (or the last recorded date in an accident book)
Health records	40 years
Safeguarding	
Where an allegation has been made about an individual, any records relating to that individual will be retained until the individual reaches the normal retirement age, or for 10 years if that is longer. This overrides any shorter retention period listed elsewhere in this table.	
DBS checks	Not kept (sight of disclosure recorded)
Volunteers	
Volunteer files	12 months following the end of volunteering.
Employees and Trustees	
Personnel files (including references, eligibility to work in the UK, sickness and absence records, disciplinary records)	6 years from end of employment (or from date of Trustee resignation)
Application form: (successful candidates)	Duration of employment
Application form: (unsuccessful candidates)	6 months after decision
Recruitment and selection materials	All candidates: 6 months after decision
References provided to others	6 years from the reference date