

DATA PROTECTION POLICY

Rationale

- 1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our employees, service users, customers, clients, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in our organisation and will provide for successful business operations.
- 1.2 The types of personal data that HOT may be required to handle include information about current, past and prospective employees, service users, customers and clients, suppliers and other third parties, and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulations 2018.
- 1.3 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.
- 1.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.
- 1.5 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.
- 1.6 This policy does not form part of your contract of employment and may be amended at any time by HOT. Where appropriate we will notify data subjects of those changes by post or email.

Roles and responsibilities

- 2.1. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change lies with the Senior Management Team.
- 2.2. The Senior Management Team is also responsible for ensuring compliance with the Act with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to your line manager.
- 2.3. Staff will not attempt to gain access to information that is not necessary to hold, know or process. All information which is held will be relevant and accurate for the purpose for

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	

which it is collected. The information will not be kept for longer than is necessary and will be kept secure at all times, in line with the Retention of Documents Policy.

- 2.4. HOT will ensure that all personal or sensitive personal information is anonymised as part of any evaluation of assets and liability assessments except as required by law.
- 2.5. Staff who manage and process personal or sensitive personal information will ensure that it is kept secure and where necessary confidential. Sensitive personal information will only be processed fairly and lawfully and in line with the provisions set out in the General Data Protection Regulations 2018 only processed in accordance with instructions set out by our Senior Management Team.
- 2.6. All members of staff are responsible for the success of this policy and you should ensure that you take the time to read and understand it. Questions regarding the content or application of Data Protection should be directed to your line manager in the first instance.

Definition of Data Protection Terms

- 3.1. **Data** – is information which is stored electronically, on a computer, or in certain paper-based filing systems (such as Family and Child Case Files).
- 3.2. **Data subjects** – for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
- 3.3. **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.
- 3.4. **Data controllers** are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act.
- 3.5. **Data processors** are employees, students, volunteers, temporary, casual, agency workers whose work involves processing personal data. Data processors must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	

- 3.6. Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- 3.7. Sensitive personal data** includes information about a person that identifies them including racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be collected with explicit consent of the person concerned and for the reason stated.

General Data Protection Regulations

- 4.1.** Anyone processing personal data must comply with the eight enforceable principles of good practice, which are explained below. These principles provide that personal data must be:
- ▶ Processed fairly and lawfully.
 - ▶ Processed for limited specifically stated purposes and in an appropriate way.
 - ▶ Adequate, relevant and not excessive for the purpose.
 - ▶ Accurate.
 - ▶ Not kept longer than necessary for the purpose it was originally collected for
 - ▶ Processed in line with data subjects' rights.
 - ▶ Kept safe and secure.
 - ▶ Not transferred to people or organisations situated in countries without adequate protection.

Fair and lawful processing

- 4.2.** The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.
- 4.3.** For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's explicit consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or if necessary to protect the vital interests of a data subject or

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	

another person where the data subject is incapable of giving consent. When sensitive personal data is being processed, additional conditions must be met.

Processing for limited purposes

- 4.4. In the course of our business, we may collect and process the personal data set out in the Schedule attached to this document (Data Processing Activities). This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).
- 4.5. We will only process personal data for the specific purposes set out in Schedule 1 or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Appropriately notifying data subjects

- 4.6. If we collect personal data directly from data subjects, we will inform them about:
 - ▶ The explicit purpose or purposes for which we intend to process that personal data.
 - ▶ The types of third parties, if any, with which we will share or to which we will disclose that personal data.
 - ▶ The means, if any, with which data subjects can limit our use and disclosure of their personal data.
- 4.7. If we receive personal data about a data subject from other sources, (Data Controllers) we will have an Data sharing agreement in place that is clear about it being their responsibility to gain explicit consent to share the information with Halifax Opportunities Trust.

Adequate, relevant and non-excessive processing

- 4.8. We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject as specified in the privacy notice.

Accurate data

- 4.9. We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data on a regular basis.

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	

Not kept longer than is necessary for the purpose (timely processing)

4.10. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required in line with the Retention of Documents Policy

Processing in line with data subject’s rights

4.11. We will process all personal data in line with data subjects' rights, in particular their right to:

- ▶ Be informed – explicit consent.
- ▶ Right to access - request access to any data held about them by a data controller (see ‘Dealing with Subject Access Requests’ below).
- ▶ To rectification - to have inaccurate data amended.
- ▶ To erasure – the right to be forgotten.
- ▶ To restrict-processing - prevent processing that is likely to cause damage or distress to themselves or anyone else.
- ▶ Data portability – obtain and re-use their own personal data for their own purposes across services.
- ▶ To object - prevent the processing of their data for direct-marketing purposes.

Security of data

4.12. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

4.13. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection/receipt to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies.

4.14. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- ▶ **Confidentiality** means that only people who are authorised to use the data can access it.
- ▶ **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- ▶ **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Where data is held electronically it should not be stored on an individual’s electronic desktop

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	

4.15. Security procedures include:

- ▶ **Entry controls** – any stranger seen in entry-controlled areas should be reported.
- ▶ **Secure lockable desks and cupboards** – desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- ▶ **Methods of disposal** – paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- ▶ **Equipment** – data users must ensure that individual monitors do not show confidential information to passers-by and that they lock (Ctrl, Alt & Delete pressed at the same time and click on lock screen) their PC when it is left unattended.

Disclosure and Sharing of Personal Information

- 5.1.** We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.
- 5.2.** We may also disclose personal data we hold to third parties:
- ▶ In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the seller or buyer of such business or assets.
 - ▶ If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.
- 5.3.** If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation we will do so, in order to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- 5.4.** We may also share personal data we hold about vulnerable children and adults where there are significant safeguarding concerns. (Refer to the Safeguarding and Protecting Children and Young People Policy and Safeguarding Vulnerable Adults Policy).
- 5.5.** We may also share personal data we hold with selected third parties for the purposes set out in the Privacy Notice.

Dealing with Subject Access Requests

- 6.1.** A Data subject must make a formal request for information we hold about the individual. This must be made in writing using a Subject Access Request Form (Appendix C).

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	



employment

children & families

learning

community & wellbeing

enterprise

inclusive integration



Employees who receive a written request should forward it to the Data Protection Officer immediately.

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy		Review Date: June 2026

APPENDIX A

Guidelines for staff regarding data protection

- (a)** Most members of staff will process personal data on a regular basis as part of their job. HOT must ensure that staff and service users, customers or clients give their consent to processing their data and are notified of the categories of processing, as required by the Act.
- (b)** Information about an individual's physical or mental health; sexual life; political or religious views; trade union membership; ethnicity or race is sensitive and can only be collected and processed with their express consent.
- (c)** Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in our Data Protection Policy. In particular, staff must ensure that records are:
 - ▶ accurate;
 - ▶ up-to-date;
 - ▶ fair;
 - ▶ kept and disposed of safely, and in accordance with our Records Retention Policy.
- (d)** Individual members of staff are responsible for ensuring that all data they are holding is kept securely.
- (e)** Members of staff must not disclose personal data, unless for normal administrative or pastoral purposes, without authorisation or agreement from the data controller, or in line with our policy.
- (f)** Before processing any personal data, all staff should consider the checklist below.

Staff Checklist for Recording Data

- ▶ Do you really need to record the information?
- ▶ Is the information 'personal' or is it 'sensitive'? If it is sensitive, do you have the data subject's explicit consent?
- ▶ Has the individual or data subject been told that this type of data will be processed?

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	

- ▶ Are you authorised to collect/store/process the data? If yes, have you checked with the data subject that the data is accurate?
- ▶ Are you sure that the data is secure? If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the data subject or the staff member to collect and retain the data?
- ▶ Have you notified the Data Protection Officer that you intend to hold the data? How long do you need to keep the data for, and what is the mechanism for review/destruction?

APPENDIX B

Guidelines for staff regarding data sharing

- (a)** The Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.
- (b)** Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- (c)** Seek advice if you are in any doubt, without disclosing the identity of the person where possible.
- (d)** Share information with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
- (e)** Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
- (f)** Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
- (g)** Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	



employment

children & families

learning

community & wellbeing

enterprise

inclusive integration



APPENDIX C

Data Subject Access Request From

Application for access to personal information

- ▶ All applicants must complete sections, 1,2 and 7.
- ▶ If you are applying on behalf of someone else, then they must complete Section 4 and you will also need to complete Section 3.
- ▶ If you are under 16 years old, then your parent, guardian or social services care manager should complete Section 5.
- ▶ If you are a parent for access on behalf of a child, please complete Section 6.

Please note: Before logging your request, we will require proof of identity by production of a passport, photo-driving licence, or a utility bill in your name and current address. Please supply proof of identity when making your application.

1. CONTACT DETAILS

Name of Applicant:

Address of Applicant:

.....

.....

Previous address if moved in the last three years:

.....

Date of Birth:

Telephone Number:

Mobile Number:

Email Address:

2. ADDITIONAL INFORMATION

To help us locate any personal information that we hold, please supply any relevant information:

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	



employment

children & families

learning

community & wellbeing

enterprise

inclusive integration



What service(s) were used or received?

.....
.....

When was the service used?

.....
.....

Please indicate the information you require:

.....
.....

Please supply any other information that you think might help us to locate your personal information:

.....
.....

3. AUTHORISATION TO ACT ON BEHALF OF THE APPLICANT

Please complete this section if you are authorised to act on behalf of the applicant.

I, (Name of Agent), have been authorised to act on behalf of:

..... (Name of person who received this service)

I declare that I will not disclose any information that I am supplied with other than to the person on whose behalf I am acting, unless they give me their express permission.

Signed (Agent): Date:

4. SERVICE USER'S AUTHORISATION

Please complete this section if an agent is acting on your behalf:

I, (Name of user of services/employee) authorise: (Name of person or agent acting on your behalf) to seek access to personal information held by Halifax Opportunities Trust. I declare that this authorisation was freely given.

Signed (Agent): Date:

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	



employment

children & families

learning

community & wellbeing

enterprise

inclusive integration



5. APPLICATION BY UNDER 16's

If you are under 16 years, a parent, guardian or Social Services Care Manager should certify that you fully understand the nature of this application and your application will then be considered:

I, (Name of parent, guardian, social worker, etc)

Address:

.....

Certify that the applicant, (Name of applicant), who is under 16 years, understands the nature of this application for access to his/her personal information.

Signed (Parent, Guardian, Social Worker, etc:)

Date:

6. PARENT APPLYING FOR ACCESS ON BEHALF OF A CHILD

If you are a parent applying for access on behalf of your child, please complete the following and tick the relevant box.

Please note that you must be able to establish that you are legally able to act on behalf of your child. This generally means that you must have parental responsibility for him or her. It should be noted that a parent can only be granted access to their child's records if this is considered to be in the child's interests.)

Name of Child: Date of Birth:

.....

.....

I (Name of parent): am making a request for access to records on behalf of the child named above and:

Tick as appropriate:

The child is incapable of understanding the request and I am making the request on his/her behalf.

The child has consented to my making this request on his/her behalf and this

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	



employment

children & families

learning

community & wellbeing

enterprise

inclusive integration



consent was freely given

Signed: Date:

(Child where consent is given)

Signed: Date:

(Parent)

7. SIGNATURE

All applicants must sign and date the following:

I wish to request access to personal information held by Halifax Opportunities Trust about:

Name of Service User:

In accordance with the General Data Protection Regulations 2018, I understand that to ensure confidentiality for us to obtain further information and to locate the information sought.

Signed: Date:

Please return this form to:

Halifax Opportunities Trust
Hopwood Lane
Halifax
HX1 5ER

Or by email to: privacy@regen.org.uk

Please note:

Halifax Opportunities Trust may contact you for further information regarding the information required.

Once the information has been collated, you will be notified that your file is ready for collection.

Information can only be disclosed once proof of identity has been seen or received.

Unique ID: HR011	Document Owner: DPO	Current Version: June 2025	Archive Period: 1 year
Master Document Kept: Cezanne	Document: Data Protection Policy	Review Date: June 2026	