Home from Home
Housing Association Ltd

Data Protection Policy and Procedure Guide

Owner: Hfh
Date: May 2025

Contents Page

Policy Statement 3

Monitoring and Continuous Improvement 4
Definitions 5
Data Protection Policy and Confidentiality Dos and Don'ts 7

Roles and Responsibilities 8

Confidentiality and Data Protection Procedure Guide 9

Introduction 9
What Information We Collect and How We Use It 9
Staff/Volunteers Personal Data 9
Customers Personal Data 9
Examples of Sensitive Data 10

How We Store Personal Data 10

With Whom and When We Share Personal Data 11

Confidentiality versus Sharing 11
Examples of Data Sharing 11
How we share information safely 12

Access Rights – How we Deal with Requests for Personal Information 12

How Long We Keep Personal Data 13

CCTV Cameras 14

Data Breaches and How to Report Them 15

Appendix 1: Home From Home Customer Privacy Notice 16

Appendix 2: Home From Home Housing Association staff / volunteers privacy notice: 2025 21

Appendix 3: Data Retention Procedures 26

Appendix 4: Legislation, Regulation and Linked Policies 27

Legislation and Regulation.....27

Other Standards/National Guideline 28

Linked Policies.....28

Document Information Sheet 29

Policy Statement

1. In order for Home from Home Housing Association (HfH) to deliver our services effectively, we need to collect and, in some cases, share information about the people we support, our staff, volunteers and our funders (our Data Subjects). Everyone we collect information from needs to be assured that we do this safely and in accordance with the law.

2. The most up to date regulation and law that this policy relates to are the European Union's General Data Protection Regulations (GDPR) most of which has been embedded within UK Law, within the Data Protection Act 2018.

3. The GDPR requires that organisations (data controllers) process personal data in accordance with the eight Data Protection Principles:

    - Fair and lawful
    - Specific to purpose
    - Adequate, relevant and not excessive
    - Accurate and up to date
    - Kept for no longer than necessary
    - Processed in accordance with data subjects' rights;
    - Kept secure;
    - Not transferred overseas without suitable safeguards.

4. We have developed an Information Asset Register and Record of how and why we process this information. Together these documents identify

    - What personal information we hold
    - Where we hold it
    - The legal basis for holding and processing the information
    - Who we share the information with
    - How we share the information and
    - How long we keep it for

5. This helps us to continuously improve on our legal obligations and minimise any potential data breaches. These documents are reviewed and updated every three years or sooner if our processes change during the year

6. All HFH staff and volunteers, consultants and/or contractors (Third Parties) engaged to carry out duties on our behalf and by our instructions will adopt and follow this policy and any related policies relating to the collection, confidentiality,

availability and integrity of our data and information, security, incident management, retention and disposal of information.

7. All data subjects have a right to be informed about how and why their data is being used. We provide this information in our 'Privacy Notices' for staff and Customers. Appendix 1 and 2

8. We have a zero-tolerance policy towards individuals who deliberately and unlawfully obtain or disclose personal data and recognise this can be a personal legal offence against this person under the General Data Protection Regulation 2018 (unlawful obtaining of personal data) which clearly states that any person must not knowingly or recklessly, without the consent of HFH as the data controller:

   - Obtain or disclose personal data or the information contained in personal data, or
   - Instruct another person to obtain or disclose the personal data or the information contained in personal data.

Embedding Policy into practice

9. To achieve our aims within this policy we will ensure that employees and volunteers fully understand and comply with these procedures within their day-to-day practice through training, monitoring and supervision. This will include as a minimum:

   - That all staff read and understand this policy and procedure guide
   - That new employees attend GDPR training during their induction period
   - That all staff undertake an e-learning refresher provided by our on-line training provider
   - Managers carry out audit checks to ensure full compliance

Monitoring and Continuous Improvement

10. This policy will be monitored by HfH's CEO and a report giving an overview of any data protection breaches will be reported to the HfH Board as and when any breaches occur. The Board will be responsible for ensuring any service improvement or learning as a result of these breaches.

Definitions

- **Data:** Information that is processed electronically or manually i.e. hard copies within filing cabinets, on a computer, e-mails, computer records, CCTV images, microfilmed documents, archived files or databases, faxes and information recorded on telephone logging systems
- **Data Breaches:** A data breach is when the information we hold, create, or share (e.g. care records) is compromised, i.e. systems hacked, incorrect information held or unavailable or out of date information required to carry out our caring role.
- **Data Controller**: A person/organisation is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files. For the purpose of this policy HFH is the Data Controller.
- **Data Processor**: A person who processes personal data on behalf of the controller. For the purposes of this policy, all staff employed by PR and some third-party contractors are data processors.
- **DPA:** The Data Protection Act 2018
- **DPIA**: Data Protection Impact Assessment
- **Data Subject**: An individual who is the subject of the personal data being kept.
- **GDPR**: General Data Protection Regulations
- **ICO**: Information Commissioner's Office, Wycliffe House, Water Lane Wilmslow, Cheshire, SK9 5AF. This is the UK's independent authority set up to promote access to official information and to protect personal information.
- **Information Governance**: Is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.
- **Personal Data**: Information relating to a living individual who can be identified from that data, and other information in the possession of the Data Controller and includes any expression of opinion about that individual
- **Privacy Notice/Notification**: The privacy notice is a written document explaining how personal information is being used, when they make contact with or use one of the organisations services. This includes why an organisation is able to process their information, the purpose of processing the data, whether it has to be provided in order to deliver the service, how long it is stored for, who it might be shared with and whether it is intended to transfer the data to another country, and whether the organisation carries out automated decision-making or profiling.
- **Processing** means obtaining, recording or holding the information or carrying out any operation on the data including organising, adapting or altering data; the retrieval, consultation or use of the data; the disclosure of the data and the

grouping, combining, blocking, erasing or destroying the data. It is difficult to imagine any activity which does not amount to processing.

- **Pseudonymisation:** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
- **Sensitive Personal Data** means personal data consisting of information as to an individual's racial or ethnic origin, political opinions, religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission of an offence or any proceedings for any offence committed or alleged to have been committed by an individual**.**

Data Protection Policy and Confidentiality Dos and Don'ts

Do

- ✓ Always ensure that personal information you collect is accurate and up to date and only keep it for as long as is necessary, for the purpose it was collected
- ✓ Review what you keep regularly to make sure it is still accurate, up to date and needed
- ✓ Explain to people why you are collecting their information and how you will be using it
- ✓ Get consent from people before sharing photographs on our web pages or in our literature
- ✓ If sharing personal data – make sure you are doing this safely e.g. encrypting information before sending
- ✓ Keep personal data secure at all times
- ✓ Always report breaches using the form in this policy.

Don't

- ✕ Use information for a different purpose than that for which it was obtained, without the consent of the person who gave it or advice from your manager.
- ✕ Disclose information to other staff members unless the use of that information is within their authorised duties
- ✕ Give out personal information over the phone or in person
- ✕ Take personal information out of the office unless you have to for work reasons
- ✕ Leave confidential information on the printer, but if you find it put copies in confidential waste bins
- ✕ Send files to your personal email account
- ✕ Do not include any sensitive personal information in any email message.

Roles and Responsibilities

Job Role	Responsibility
Board Members	Board members are responsible for overseeing compliance of this Policy and Procedure Guide and reporting to the main HfH Board
Chief Executive	The Chief Executive has overall responsibility for overseeing compliance with this policy and procedure guide.
Housing Manager	Is responsible for ensuring all staff, contractors and volunteers fully comply with this policy and procedure guide and Responsible for ensuring that employees attend the appropriate level of training for their role and must Report all Data Protection Breaches to the CEO
Housing Officer/volunteers/Contractors	Are responsible for complying with this policy and procedure guide and Report any data protection breaches to managers immediately HfH staff/volunteers must complete all appropriate training and competency assessments

Confidentiality and Data Protection Procedure Guide

Introduction

This procedure guide will help staff and volunteers understand the types of information we need to collect to carry out our services, the legal reasons for collecting this information and where we can store information safely. It will also cover when consent is required for certain pieces of information, who we can share the information with and why, how to share information safely and how long we can keep information for.

What Information We Collect and How We Use It

1. Some examples of types of personal data that we collect and process are detailed below (non-exhaustive list).

2. The legal reasons for collecting and processing this data are detailed in Appendix 3 Section 6 of the GDPR. Where the data is classed as 'sensitive data' we also need to identify a further legal reason for processing this data, see Appendix 4 Section 9 of the GDPR.

Staff/Volunteers Personal Data

- Names and addresses
- Email Addresses
- National Insurance Number
- Bank Details
- Employment Application Form
- Employment Offer Letter
- Staff Contract
- Pay Slip
- Supervision Notes
- Appraisal, Disciplinary Records
- Staff Handover Sheet
- Disclosure and Barring Service Check
- CCTV Image (if applicable)
- Driving Licence (if applicable)
- Reference Request

Customers Personal Data

- Names and addresses
- Application Forms
- Needs Assessment (if applicable)
- Risk Assessment (if applicable)

- CCTV Image (if applicable)
- Safeguarding Referrals (if applicable)
- Medical Records (if applicable)

Examples of Sensitive Data

- Criminal Record Data

How We Store Personal Data

1. Article 5 (1. f.) of the GDPR states that we must ensure that data is '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'

2. Fundamentally we hold personal data in two main ways – within paper documents, stored in filing cabinets and also within computer software. The latter includes all data stored on computers, laptops, memory sticks, mobile phones and any other mobile IT equipment that we use.

3. Information is stored within software for different reasons.

- Payroll software,
- Accounting Software.
- Microsoft office for our software applications e.g. word, excel, powerpoint etc
- Any others?

4. We have checked that all of our software providers have robust security measures compliant with all Data Protection legislation and regulation.

Commented [KP1]: This may be an action for you

5. All third parties that hold information on our behalf about staff, funders, volunteers, Customers, are also required to take appropriate security measures to ensure that their data protection processes are safe from data breaches. Third parties are required to read and sign the Contract in Appendix 6 to evidence that they are compliant with all UK Data Protection legislation.

6. All staff must ensure that they only have access to information, IT and manual files, that they need to hold in order to carry out their work.

7. Within shared offices or offices that Customers can access, all staff must ensure that they have a screen saver on their computers and that no personal data is left on desks or posted on walls within office spaces. Personal data should also not be displayed around the HFH building.

8. All staff must ensure that any paper documentation is shredded when there is no further need for the information to be held (Appendix 7 Data Retention Guidance)

9. Never store personal data about a client/other staff members/funders on your personal mobile equipment unless it is stored within our secure portals e.g. People Planner

10. If working from home, ensure all personal data is kept away from other members of your family, friends and guests

With Whom and When We Share Personal Data

Confidentiality versus Sharing

1. It is essential that we treat personal data with the highest levels of confidentiality. However, there are times when we may need to share people's data. The following are examples when we have to do this.

Examples of Data Sharing

2. Under the GDPR relevant personal **information can be shared** lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being. We may not need to get a person's consent to share their data under these circumstance (see section on Consent below).

3. The Data Protection Act 2018 also sets out the lawful grounds for processing of special category personal data, including without consent if the circumstances justify it, where it is in the substantial public interest to safeguard children and individuals at risk.

4. Effective information-sharing underpins joint working and is a vital element of both early intervention and safeguarding.

5. **Consent**: We may need to ask people for their consent to share their personal information, for example when we want to use a person's picture on any of our promotional materials such as leaflets or on our website. We will always seek agreement from the person whose data we are sharing prior to doing this.

6. However, we don't always need to ask people for their consent to collect and process their information, if we are collecting their data for other legal reasons (see 9 below). We will however provide people with Privacy Notifications (Appendix 1 and 2) where this is the case.

7. Where we do need to ask for consent, we do this by asking them to complete a consent form. An example template to use is provided in Appendix 6 of this policy document.

8. The following provides examples of data we may need to share which **does not require consent** as there are other legal reasons for sharing this information.

9. We have a legal obligation to share information with local authority safeguarding leads, or the police if they there is a danger to a person's (i.e. staff, client, volunteer) life or a criminal act is taking place.

10. Data is shared with third parties who manage our databases and administrative systems in order to obtain pre-employment references from other providers, obtain assessments as part of a recruitment process, obtain employment background checks from third – party providers and necessary criminal records checks from the Disclosure and Barring Service.

11. We also share staff data with third parties that process data on our behalf for example in connection with insurances and legal advice, employee relations matters, payroll, the provision of benefits i.e. pensions benefits and occupation health services if and when used.

12. We may also need to be share staff data with third parties in the context of a potential TUPE transfer if we are taking on a new service

How we share information safely

13. When we share information with a third party, we will ensure that it is carried out safely and securely to minimise any data breaches. Staff will consider the following:

- Only share the information that they need to share.
- When sending information by email– always consider whether using pseudonyms, for example initials, can be used rather than a person's full name.
- When employees send information by email both internally and externally, you must ensure that the email is encrypted i.e. by password protecting the document and sending the password in a follow up email or texting the person by phone.

Access Rights – How we Deal with Requests for Personal Information

1. Under the Section 7 of the Data Protection Act 2018 anyone whom we collect and process personal data about, has a right to make a Subject Access Request (SAR) to request information about the personal data that we hold about them.

2. At HFH we accept data requests in written or email format.

3. We will respond to the SAR within one month of receiving the request in accordance with the Information Commissioners Office requirements. We may extend the time to respond by a further two months if the request is complex or

we have received a number of requests from the same individual, e.g. other types of requests relating to individuals' rights

4. There are some exemptions to the data we can provide. This includes the following:

- Employment References sent to other organisations (but not received for new employees)
- If an enactment requires an organisation to make information available to the public, any personal data included in it is exempt from the right of subject access.
- Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access. These purposes are:
    - the prevention or detection of crime;
    - the capture or prosecution of offenders; and
    - the assessment or collection of tax or duty
- Personal data that is processed for management forecasting or management planning e.g. restructuring/re-organisational plans
- Where personal data includes information about a person's health provided by a third party e.g. doctor, psychiatrist, counsellor unless you have the permission of the third-party provider
- Special rules apply where providing subject access to information about an individual's physical or mental health or condition are likely to cause serious harm to them or to another person's physical or mental health or condition
- Exemptions apply where the information includes personal data of another Customers/member of staff/member of the public
- Some exemptions are for organisations who carry out a statutory function if it is likely that providing the information will prejudice the proper discharge of these functions

For more information on access rights, refer to the Information Commissioners guidance in the link below[1]:

How Long We Keep Personal Data

1. Under the Data Protection Act personal data should 'not be kept for longer than necessary'.

2. A detailed guidance of long we keep information for is provided in Appendix 3.

[1] https://ico.org.uk/media/for-organisations/documents/2259722/subject-access-code-of-practice.pdf

CCTV Cameras

1. HFH operates a number of CCTV Cameras around our head office. The purpose of the cameras is as follows: -

    - To prevent and detect Crime and anti-social behaviour
    - To ensure public Health and Safety

2. In doing so we must comply with our obligations under the Data Protection Act. We do this by ensuring the following:

3. CCTV cameras are not places in areas which are not of interest and these areas are not intended to be the subject of surveillance

4. Only in exceptional cases and where necessary to deal with serious concerns will we place cameras in areas where people have a heightened expectation of privacy (for example in bedrooms etc). In these cases, extra efforts are made to ensure that those under surveillance or their advocates if they lack capacity are aware of the cameras and have provided consent to have them installed. We will never install cameras in bathrooms or toilets.

5. We will not use CCTV to record audio (for example, conversations between members of the public) as this is highly intrusive

6. There is restricted access to recorded material and recorded images are viewed only by the CEO in a private location.

7. Images obtained using CCTV are not used for any purpose other than the reason they were originally captured.

8. Please note that Customers have the right to request images recorded of them. Such requests should be dealt with formally as Subject Access Requests.

9. We do not generally release CCTV Images to third parties (except for exemptions when we need to share personal data – see section above on information sharing).

10. Staff must always follow the guidelines above and for new staff carry out the following:

Commented [KP2]: Delete if not applicable

- When first showing new Staff around HFH, you must let staff know they are in an area where CCTV cameras are operational, and that CCTV Cameras are recording their personal data.
- You should also provide an explanation of why CCTV cameras are in operation (i.e. the purpose of the camera) and what they are used for.

Data Breaches and How to Report Them

What is a data breach?

1. A data breach can be in any of the following 3 ways:

Confidentiality – When a person gains access to information they shouldn't have. This might be malicious i.e. a hacker, or it might be a simple mistake i.e. sending an email to the wrong person.

Integrity – we need to know that information is accurate and that it was created by the right person. If there is an error on the sheet – whether on purpose or not – this is a data breach; or

Availability – for data to be useful we need to be able to access it. If it isn't available this is also a breach, e.g. staff records should be kept securely in a locked office/locked filing cabinet but if the keys go missing and no one can access that record then this is a data breach.

What should you do if there is a data breach or you think there is a data breach?

2. It is better to report a breach even if you are not sure that it is one. As with incident reporting, near misses are as important to report as actual incidents. This is how we learn and can hopefully prevent these things happening in the future.

3. If you believe a crime has been committed, someone has been injured, or an intruder is on site contact the emergency services via 999.

4. Fill out the Data Security Incident Report Form provided in Appendix 8. This form should then be handed to the HFH Data Security and Protection Lead**.** Currently this is

Commented [KP3]: Please state who this may be

5. If you have identified a potential security breach, inform a HFH Manager or HFH's Data Security and Protection Lead at the earliest opportunity.

Appendix 1: Home From Home Customer Privacy Notice

Registered name: Home From Home Housing Association
This privacy notice tells you what to expect us to do with your personal information.

- Contact details
- What information we collect, use, and why
- Lawful bases and data protection rights
- Where we get personal information from
- How long we keep information
- Who we share information with
- How to complain

Contact details

Home From Home Housing Association, 230 Portway, , LONDON, , E15 3QY, GB
020 8472 7711
mail@hfhhousing.org

What information we collect, use, and why

We collect or use the following information to **provide housing services and support services to you:**

- Names and contact details
- Gender
- Pronoun preferences
- Addresses
- Date of birth
- Emergency contact details
- Next of kin details
- Information about work, home and living conditions
- Information about support requirements
- Criminal offence data
- Records of meetings and decisions
- Information about income and financial needs for funding or personal budget support
- Information relating to compliments or complaints

We also collect or use the following information to **provide housing and support services to you**:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Health information

We collect or use the following information to **receive donations or funding and organise fundraising activities**:

- Names and contact details
- Addresses
- Payment or banking details

We collect or use the following personal information to **comply with legal requirements**:

- Name
- Contact information
- Identification documents

We collect or use the following personal information for **dealing with queries, complaints or claims**:

- Names and contact details
- Address
- Witness statements and contact details
- Relevant information from previous investigations
- Information relating to health and safety (including incident investigation details and reports and accident book records)

Lawful bases and data protection rights

Under UK data protection law, we must have a "lawful basis" for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO's website.
Which lawful basis we rely on may affect your data protection rights which are in brief set out below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:

- **Your right of access** - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not

receive all the information you ask for. You can read more about this right here.

- **Your right to rectification** - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. You can read more about this right here.
- **Your right to erasure** - You have the right to ask us to delete your personal information. You can read more about this right here.
- **Your right to restriction of processing** - You have the right to ask us to limit how we can use your personal information. You can read more about this right here.
- **Your right to object to processing** - You have the right to object to the processing of your personal data. You can read more about this right here.
- **Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. You can read more about this right here.
- **Your right to withdraw consent** – When we use consent as our lawful basis you have the right to withdraw your consent at any time. You can read more about this right here.

If you make a request, we must respond to you without undue delay and in any event within one month. To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

Our lawful bases for the collection and use of your data

Our lawful bases for collecting or using personal information to **provide housing and support services** are:

- Consent - we have permission from you after we gave you all the relevant information. All your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Legal obligation – we must collect or use your information so we can comply with the law. All your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Our lawful bases for collecting or using personal information to **receive donations or funding and organise fundraising activities** are:

- Consent - we have permission from you after we gave you all the relevant information. All your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

Our lawful bases for collecting or using personal information to **comply with legal requirements** are:

- Legal obligation – we must collect or use your information so we can comply with the law. All your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Our lawful bases for collecting or using personal information for **dealing with queries, complaints or claims** are:

- **Consent** - we have permission from you after we gave you all the relevant information. All your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

Where we get personal information from

- Directly from you
- Local Authorities
- Social Services/Mental Health Services

How long we keep information

For information about how long we keep your data - please ask to see our Data Protection Policy.

Who we share information with

Others we share personal information with

- Social Services
- Organisations we need to share information with for safeguarding reasons
- Professional advisors

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.
If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113
Website: https://www.ico.org.uk/make-a-complaint

Updated April 2025

Appendix 2: Home From Home Housing Association staff / volunteers privacy notice: 2025

Registered name: Home From Home Housing association

We are the controller of your personal data. For more information on controllers and their responsibilities please see the ICO's guidance on Key data protection terms you need to know.

This privacy notice tells you what to expect us to do with your personal information when you work for us.

- Contact details
- What information we collect, use, and why
- Lawful bases and data protection rights
- Where we get personal information from
- How long we keep information
- Who we share information with
- How to complain

Contact details

Home From Home Housing Association, 230 Portway, LONDON, E15 3QY, Tel: 020 8472 7711
Email: mail@hfhhousing.org

What information we collect and use, and why

Staff recruitment, administration and management

We collect or use the following personal information as part of **staff recruitment, administration and management**:

- Contact details (e.g. name, address, telephone number or personal email address)
- Date of birth
- National Insurance number
- Gender
- Copies of passports or other photo ID
- Copies of proof of address documents (e.g. bank statements or bills)
- Marital status

- Next of kin or emergency contact details
- Employment history (e.g. job application, employment references or secondary employment)
- Education history (e.g. qualifications)
- Right to work information
- Details of any criminal convictions (e.g. DBS checks)
- Political, conflict of interest or gift declarations
- Performance records (e.g. reviews, disciplinary records, complaints or disciplinary action)
- Training history and development needs
- Monitoring employees' IT use

We also collect the following information for **staff recruitment, administration and management**:

- Racial or ethnic origin
- Trade union membership

Salaries and pensions

We collect or use the following personal information as part of **managing salaries and pensions**:

- Job role and employment contract (e.g. start and leave dates, salary, changes to employment contract or working patterns)
- Time spent working (e.g. timesheets or clocking in and out)
- Expense, overtime or other payments claimed
- Leave (e.g. sick leave, holidays or special leave)
- Maternity, paternity, shared parental and adoption leave and pay
- Pension details
- Bank account details
- Payroll records

We also collect the following information for **managing salaries and pensions**:

- Racial or ethnic origin
- Trade union membership

Lawful bases and data protection rights

Under UK data protection law, we must have a "lawful basis" for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO's website.

Which lawful basis we rely on may affect your data protection rights which are set out in brief below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:

- **Your right of access** - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. You can read more about this right here.
- **Your right to rectification** - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. You can read more about this right here.
- **Your right to erasure** - You have the right to ask us to delete your personal information. You can read more about this right here.
- **Your right to restriction of processing** - You have the right to ask us to limit how we can use your personal information. You can read more about this right here.
- **Your right to object to processing** - You have the right to object to the processing of your personal data. You can read more about this right here.
- **Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. You can read more about this right here.
- **Your right to withdraw consent** – When we use consent as our lawful basis you have the right to withdraw your consent at any time. You can read more about this right here.

If you make a request, we must respond to you without undue delay and in any event within one month.

To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

Our lawful bases for the collection and use of your data

Our lawful bases for collecting or using personal information as part of **staff recruitment, administration and management** are:

- Consent - we have permission from you after we gave you all the relevant information. All your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Contract – we must collect or use the information so we can enter into or carry out a contract with you. All your data protection rights may apply except the right to object.
- Legal obligation – we must collect or use your information so we can comply with the law. All your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.
- Public task – we must collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours. All your data protection rights may apply, except the right to erasure and the right to portability.

Our lawful bases for collecting or using personal information as part of **managing salaries and pensions** are:

- Contract – we must collect or use the information so we can enter into or carry out a contract with you. All your data protection rights may apply except the right to object.
- Legal obligation – we must collect or use your information so we can comply with the law. All your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Where we get personal information from

We collect your information from the following places:

- Directly from you
- Employment agency
- Schools, colleges, universities or other education organisations
- Referees (external or internal)

- Pension administrators or government departments (e.g. HMRC and DWP)
- Public sources (e.g. LinkedIn or other websites)

How long we keep information

For more information on how long we store your personal information or the criteria we use to determine this please contact us using the details provided above.

Who we share information with

In some circumstances, we may share information with the following organisations:

- Training suppliers
- HMRC
- External auditors

Data processors

We use the following data processors for the following reasons:

Human Resources, Training Organisations, Finance, Software providers
The data processors carry out the following activities for us: Process our payroll manage our IT systems, provide training.

Commented [KP4]: any other external data processors -

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113 and Website: https://www.ico.org.uk/make-a-complaint

Appendix 3: Data Retention Procedures

There are currently no statutory requirements on the length of time we might be expected to retain personal data that covers housing or supported housing and nothing is specified within the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010, Regulator of Social Housing Standards or the Care Act 2014.

Home From Home has therefore chosen to adopt the guidelines as set out within the 'Records Management Code of Practice for Health and Social Care 2016', as these guidelines established on the basis of legal compliance and best practice.

The Chartered institute of Personnel & Development also produce a comprehensive and useful factsheet in relation to statutory requirements on the retention of information which also informs our policy

The table below sets out the time period for retaining different records after the last entry made or the end of the tenancy/placement/ or service. These rules relate to all paper and digital records held within computer files/folders.

Customer Records Retention

3 YEARS	**8 YEARS**
Deceased Customers: (Unless there is an outstanding legal investigation taking place in relation to the persons death).	Customer Register
	Customers Personal Finance Records including all benefit applications and receipts
	Record of appointments
	Tenancy Agreements and Allocation records
	Signing In / out books (if applicable)
	Communication/feedback books (if applicable)
	Record of signatures and initials
	Needs assessments, support plans, risk assessment, (if applicable)
	Incidents and Accidents
	Medication records (if applicable)
	All health records (if applicable)
	Use of physical intervention and record of actions (if applicable)
	Complaints and actions taken

Employee Retention of Information

Employee Data Type	Retention Approach	Minimum Time
Applications - Successful	Retain whilst employed and for designated period afterwards	7 years
Personal development data	Retain whilst employed and for designated period afterwards	7 years
Sickness and medical records	Retain whilst employed and for designated period afterwards	7 years
Personal and Payroll data	Retain whilst employed and for designated period afterwards – as financial info contained, retain longer	HMRC say 3 years plus current year
Pension data	Retain whilst employed and for designated period afterwards	6 years in keeping with Payroll data
Applicants - unsuccessful	Dispose of short time after end of recruitment process	6 months

Appendix 4: Legislation, Regulation and Linked Policies

Legislation and Regulation

- Regulator of Social Housing's regulatory framework
- Data Protection Act 2018
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- EU General Data Protection Regulations 2018
- National Data Guardian Standards 2018

Other Standards/National Guideline

- The Information Commissioners Codes of Practice
- National Housing Federation Code of Practice
- The Common Law Duty of Confidentiality
- https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care/hscic-guide-to-confidentiality-references/section-2
- https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf

Linked Policies

- Safeguarding Adults and Children Policy and Procedure
- Incident Reporting and Management Policy and Procedure
- Support Planning Policy and Procedure
- Complaints Policy

Document Information Sheet

Policy or Procedure Title	Data Protection Policy and Procedure
Version and Active Date	Version: 01 Date: 03/05/2025
Document Owner	Hfh
Consultation with HfH Customer Scrutiny Panel	
Review Frequency	At least every 2 Years
Date of Last Review	
Date of Next Review	03/05/2027