

# Information Governance Policy

## 1.0 Introduction

1.1 We hold personally identifiable information (Personally Identifiable Information) about our customers, employees, involved residents, suppliers and other key stakeholders, and use this to carry out our business and deliver our corporate objectives. We will implement appropriate technical and organisational measures to ensure that processing is performed in accordance with our legal obligations.

1.2 This policy describes our approach to information governance and details the measures we have taken to ensure Personally Identifiable Information is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what we need to deliver efficient and effective services
- Accurate and up to date - inaccurate Personally Identifiable Information will be deleted or corrected without delay
- Kept in a form which allows for Data Subjects to be identified for no longer than is necessary
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, damage or destruction through the use of technical and organisational measures.

1.3 This policy forms part of the terms and conditions of your contract of employment, any breach regarded as misconduct may lead to disciplinary action under the appropriate disciplinary procedure.

## 2.0 Compliance Requirement

2.1 The objective of this policy is to ensure compliance with all relevant data protection and information security legislation:

- Data Protection Act 2018 (DPA)
- General Data Protection Regulation (GDPR)
- Privacy and Electronic Communications Regulations (PECR)

## 3.0 Responsibilities

3.1 The **Data Protection Officer (DPO)** is responsible for ensuring this policy and supporting practice meets compliance requirements. The DPO's responsibility consists of setting standards and practice for:

- Adequate protection of data from unauthorised access
- Maintenance of high quality data

- Capturing and processing data relevant and limited to what we need to deliver efficient and effective services
- Producing and maintaining a Data Retention Matrix (DRM) - making this available to employees
- Maintaining our privacy notice, ensuring it is fit for purpose, enabling data subjects to be made aware of how their Personally Identifiable Information is being processed
- Responding to, investigating, and reporting on breaches, near-misses, and data subject access requests including liaison with the Information Commissioners Office (ICO)
- The controlling, processing, sharing, disposal and destruction of data
- Provision of data agreement documentation enabling the organisation to ensure data processors understand their responsibilities regarding information security and data protection
- Monitoring the organisations performance and compliance against our Measures of Effectiveness, instigating lessons learned and improvement action as required
- Inputting to, and quality assuring, learning content for Beyond colleagues

3.2 **Senior Leaders** are accountable for ensuring their service areas are compliant with the standards set out in this policy covering:

- Protection of data from unauthorised access
- Maintaining the quality of service area data
- Capturing and processing data relevant and limited to what is needed to deliver efficient and effective services ensuring any change is reflected within the Information Asset Register
- Valid data agreements are in place where required
- The secure disposal and/or destruction of data
- Ensuring that data stored is compliant with the Date Retention Matrix (DRM)
- Where applicable, ensuring data subjects are made aware of how their Personally Identifiable Information is being processed
- The reporting of breaches and near misses to the DPO
- Responding in a timely manner to Data Subject Access Requests (DSAR's)
- Collaborating with the DPO to identify, agree, and implement lessons learned in pursuit of compliance
- Ensuring employees have completed mandatory learning for Information Governance & Data Protection
- Promoting and supporting the role of the service area Data Protection Champion (DPC) and ensuring there is DPC continuity

3.3 **Data Protection Champions** are responsible for:

- Maintaining their designated service areas Information Asset Register and notifying the DPO of any change
- Maintaining a record of Data Agreements and their validity ensuring steps are taken to enable compliance, seeking expertise from the DPO where required
- Identifying opportunities for improving service area data quality, governance and protection practices and promoting best practice

### 3.4 **Employees** are responsible for:

- Securing and maintaining the quality of data
- Reporting data breaches to their line manager, senior leader, DPC, and DPO
- Complying with privacy notices, data agreements, data retention matrix and the Information Governance policy in general
- Taking steps to ensure mandatory learning is valid and complete

## 4.0 **Sustainability**

4.1 Wherever possible, data will be stored electronically as we increasingly move away from traditional, paper-based resources. This policy does, however, apply to Personally Identifiable Information (Personally Identifiable Information) in all forms, including:

- Paper based materials
- Information stored electronically on information systems, whether deployed or accessed on or off site. Note, email should not be used for document/data storage.
- Information stored on our computer network
- Corporate information stored on any hardware, including mobile devices and removable media. See ICT Policy in relation to using removable media/hardware.
- Electronic recording devices, including video, cameras, audio and CCTV systems
- Information transmitted via telephone, voicemail, and/or post
- Any other data we control or process.

## 5.0 **Standards**

### 5.1 **Lawfulness of processing & data protection by design and default**

5.1.1 We will identify our legal bases for processing Personally Identifiable Information within our privacy notice and make this available to data subjects. We will ensure at least one of the following principles applies to all of our processing activities:

- a. The data subject has given consent to the processing of their Personally Identifiable Information for one or more specified purposes. Please note the vast majority of our processing does not rely on consent, however where it does we will ensure we can clearly demonstrate this was provided freely and how this can be withdrawn. Where services are offered to children (below the age of 16) we will ensure that consent is given by the person who holds parental responsibility over the child
- b. Processing is necessary for the performance of a contract to which the data subject is a party, for example a tenancy agreement, contract of employment or service level agreement
- c. Processing is necessary for compliance with a legal obligation, for example, RIDDOR reporting
- d. Processing is necessary in order to protect the vital interest of the data subject or another natural person
- e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- f. Processing is necessary for the purposes of our legitimate interests or by the freedoms of the data subject which require protection of Personally Identifiable Information (particularly where the data subject is a child).

5.1.2 We embrace data protection by design and by default; before collecting Personally Identifiable Information we will consider why we need it, what is being requested, how it will be used and how long we need to keep it for. Our Data Retention Matrix sets out how long data should be retained for - this is maintained by the organisations Data Protection Officer and can be found on the intranet. We will adopt a risk-based approach when implementing technical and organisational measures to protect the rights of data subjects.

5.1.3 We will only process special category data where at least one of the following applies:

- a. The data subject has given explicit consent
- b. Processing is necessary for the purposes of carrying out our obligations or exercising specific rights in terms of employment and social security and social protection law
- c. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- d. Processing is carried out in the course of our legitimate activities (with appropriate safeguards) as a not-for-profit body
- e. Processing relates to Personally Identifiable Information which is made public by the data subject
- f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- g. Processing is necessary for reasons of substantial public interest
- h. Processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes.

## **5.2 Privacy notice and confidentiality**

5.2.1 We will produce and maintain a privacy notice and ensure that this is made available to data subjects. Our privacy notice will provide the following information:

- a. The types of data we hold on data subjects and how these are processed
- b. Our legal bases for processing Personally Identifiable Information
- c. How Personally Identifiable Information is managed and when it may be shared with third parties
- d. The recipients or categories of recipients of Personally Identifiable Information (if any)
- e. Rights of the data subject and how these can be exercised
- f. The identity and contact details of our data protection officer
- g. Details of any revisions and the date the privacy notice was last updated.

5.2.2 We will also provide data subjects with the following further information:

- a. The length of time that Personally Identifiable Information will be stored, or the criteria used to determine this period
- b. Whether the provision of Personally Identifiable Information is a statutory or contractual requirement, or necessary to enter into a contract, and the possible consequences should a data subject refuse to provide such data
- c. The existence of automated decision-making, including information on the logic involved and the significance and consequences of such processing (where applicable).

### 5.3 Data processing

- 5.3.1 All users of our information systems must be formally authorised to do so and have signed our ICT policy. Employees are granted access to data that they need in order to fulfil their roles and responsibilities and must not pass this onto others unless they have been granted the appropriate authorisation to do so.
- 5.3.2 We will only share Personally Identifiable Information with external organisations if there is a legal obligation for this to be shared, there is a valid exemption contained within the Data Protection Act 2018 or a valid data sharing or data processing agreement exists. We will take steps to ensure that data is transferred in a secure manner, including:
- a. Password protecting all electronic records that contain Personally Identifiable Information (if a password needs to be shared this should be sent separately)
  - b. Special category data will only be exchanged through the Criminal Justice Secure email (CJSM) system or similar.
  - c. When exchanging information via email or fax, recipient addresses will be checked carefully prior to transmission
  - d. Using BCC rather than CC when emailing multiple data subjects to avoid sharing email addresses and other Personally Identifiable Information
  - e. Unsolicited communications requesting information which is not unclassified should not be acted upon until (and unless) the source of the communication has been verified
  - f. Employees must not disclose or copy data which is not unclassified unless a valid data sharing or data processing agreement is in place, or until they are authorised to do so.
- 5.3.3 We operate a clear desk policy, and employees must ensure that any records containing Personally Identifiable Information are protected and out of sight before leaving their workstation (this includes vehicles). Personally Identifiable Information must not be stored on general access drives; when stored electronically on team drives records should be password protected to control access.
- 5.3.4 Computer screens should be positioned in a way so that they cannot be viewed by unauthorised persons and all electronic devices should be locked whilst unattended.
- 5.3.5 Personally Identifiable Information that we have collected must not be processed on personally owned devices.
- 5.3.6 Employees are not given rights of privacy in relation to their use of our data and information systems. The ICT team may access or monitor personal data contained in any of our information systems, including mailboxes, web access logs or file stores.
- 5.3.7 We will classify our data based on the extent that it needs to be controlled:



Confidential

Data we have a legal obligation to keep securely stored.



Restricted

Data that is provided on a 'need-to-know' basis and is not freely available in the public domain.



Unclassified

Data that is freely available or can be shared with other parties, both internal and external.

5.3.8 We will maintain an information asset register that provides full details of all our processing activity, together with any technical and organisational steps we have taken to ensure the security of Personally Identifiable Information.

5.3.9 Confidential, paper records must be disposed of using the confidential waste bins or shredder provided. Removable storage, for example USB memory sticks, DVDs/CDs and media cards must be passed to the ICT team for secure disposal or reformatting.

#### **5.4 Data subject access requests (DSAR)**

5.4.1 Data subjects can exercise their right to request their Personally Identifiable Information on the submission of a written request to the data protection officer. This will be processed free of charge, unless deemed to be 'manifestly excessive'; where this is the case an appropriate processing fee will be applied (as determined by the data protection officer).

5.4.2 On receipt, we will provide the requested information without delay and at least within one month of receipt of the request. This period may be extended by two further months if necessary, taking into account the complexity of the request. We will inform the Data Subject of any such extension within one month of receipt of the request, together with reasons for this and their option to lodge a complaint with the Information Commissioner.

5.4.3 Where the data subject makes their request by electronic form, we will respond electronically unless otherwise requested. Where Personally Identifiable Information is sent in hard copy, this will be done as a recorded delivery and all copies stamped to evidence that they relate to a DSAR.

#### **5.5 Data breach reporting**

5.5.1 In the case of a data breach, we will notify the Information Commissioner within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects. Where a report is required, we will include at least the following information:

- a. The nature of the breach including where possible the categories and approximate number of data subjects and Personally Identifiable Information concerned
- b. The name and contact details of the data protection officer
- c. The likely consequences of the breach
- d. The steps we have taken, or propose to take, to address the breach.

5.5.2 We will document all data breaches and report these, together with significant near misses, to our Audit and Risk Committee, taking action to mitigate risk where necessary

5.5.3 When the breach is likely to result in a high risk to the rights and freedoms of data subjects, we will notify them without undue delay. We will not need to notify data subjects where the lost data

has been encrypted, or where we have taken subsequent measures which ensure the risk is no longer likely to materialise. We will utilise our website and social media channels to make a statement about a data breach where it is impractical to notify data subjects individually.

## 5.6 Data privacy impact assessment (DPIA)

5.6.1 Where we introduce a new policy, initiative, or there is a significant change in an operating environment that is likely to result in a high risk to a data subject's rights and freedoms we will carry out a DPIA. This will contain at least:

- a. A description of the processing operation, its purpose and the legal bases for processing
- b. A risk based assessment of the intended processing
- c. The measures that will be taken to address risk, including safeguards, security measures and mechanisms to ensure compliance with our legal obligations.

5.6.2 We will consult with the Information Commissioner whenever a DPIA indicates processing would result in a high risk following the introduction of planned controls.

## 5.7 Data Quality

5.7.1 In order to deliver effective and efficient services we will endeavour to maintain high quality data ensuring data is accurate, up to date, captured objectively, and complete.

5.7.2 Where a data subject reports inaccuracy in the personal data we hold (or we identify it), it is to be corrected and confirmed with the data subject. Other recipients of the data will be notified where required.

## 6.0 Consultation

6.1 Senior leaders and data protection champions will be consulted.

## 7.0 Review

7.1 This policy will be reviewed every three years, or sooner, if triggered by changes in regulation, legislation or business need.

## 8.0 Definitions

8.1 **Personally identifiable information:** Any data, either in isolation or contained within a record, that could potentially identify an individual, including information which could distinguish or trace their identity. Examples of Personally Identifiable Information include (but are not limited to):

- Name, address and other contact details (telephone number, email address)
- Date of birth
- National Insurance number
- Employee or customer number
- Photograph / Video

- 8.2 **Special category data:** Personally Identifiable Information that may be classed as 'sensitive', for example:
- Financial information (bank account details, benefit eligibility etc.)
  - Race or ethnic origin
  - Political opinion
  - Sexual orientation
  - Religious (or other similar) beliefs
  - Trade union membership
  - Details relating to an individual's physical or mental health.
- 8.3 **Data:** Raw facts gathered about someone or something. Data needs to be processed in order to create information, which may then be stored within a record.
- 8.4 **Record:** Processed data that has been placed into a digital or physical location, for example, a tenancy agreement, contract of employment or database. A record will contain many different categories or processed data.
- 8.5 **Data subject:** An identified person, or a person who can be identified (either directly or indirectly) through the application of Personally Identifiable Information or special category data.
- 8.6 **Data controller:** The entity that, either alone or jointly with others, determines the purpose, conditions and means of processing Personally Identifiable Information.
- 8.7 **Data processor:** The entity that processes Personally Identifiable Information on behalf of the data controller. We will only use data processors who can provide sufficient guarantees on their data protection practices.
- 8.8 **Data protection officer (DPO):** The person who is responsible for making sure that Information Governance and Data Protection Policy standards are set and maintained, providing advice and guidance with regard data protection obligations. Information about Beyond Housings DPO can be found on our intranet and the company website.
- 8.9 **Data recipient:** The entity to whom Personally Identifiable Information is disclosed, including any third parties.
- 8.10 **Processing:** Any operation performed on Personally Identifiable Information, including (but not limited to) collection, recording, organising, structuring, storage, adaption, retrieval, consultation, use, disclosure, alignment or erasure.
- 8.11 **Data subject access request (DSAR):** a right of data subjects to find out what Personally Identifiable Information we hold about them, why we hold it and who we disclose it to. DSARs must be responded to within one month and any information provided free of charge (unless a request is deemed to be 'manifestly excessive').



- 8.12 **Manifestly excessive:** DSARs may be defined as ‘manifestly excessive’ due to their repetitive character or if they would cause significant technical difficulties. The decision as to whether a request is ‘manifestly excessive’ will be taken by the data protection officer.
- 8.13 **Data breach:** A breach of security that has resulted in the accidental destruction, loss, alteration, unauthorised disclosure of or access to Personally Identifiable Information.
- 8.14 **Profiling:** Any form of automated processing of Personally Identifiable Information to evaluate personal aspects of a data subject, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interest, reliability, behaviour, location or movements.
- 8.15 **Pseudonymisation:** The processing of Personally Identifiable Information in such a way that it can no longer be linked to a data subject without the use of additional information, kept separately.
- 8.16 **Confidential:** Data that we have a legal obligation to keep securely stored, for example employee HR records.
- 8.17 **Restricted:** Data that is provided on a ‘need to know’ basis and not freely available in the public domain, for example, invoices and credit card request forms.
- 8.18 **Unclassified:** Data that is freely available and can be shared with other parties, both internal and external, for example performance scorecards.
- 8.19 **Measures of Effectiveness:** Measures of Effectiveness are concerned with ensuring the necessary controls and metrics are in place enabling an understanding of performance/compliance. Measures of Effectiveness category considerations encompass Management Controls, Business Processes, Operational Controls, and Technical Controls.
- 8.20 **Data Quality:** Capturing data accurately and objectively, ensuring reasonable steps are taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or corrected without delay.
- 8.21 **Information Asset Register:** An information asset register is a list of personal information assets held by an organisation. It is a mechanism for understanding and managing an organisation’s assets and the risks to them; including the links between the information assets, their business requirements and technical dependencies.
- 8.22 **Data Retention Matrix:** The Data Retention Matrix specifies the retention and destruction requirements that apply to all information, personal and non-personal, held by the Company regardless of the form they take i.e. paper, electronic records, removable media etc. This includes, but is not limited to, letters, emails, financial information (such as statements or invoices), reports, legal documents (such as contracts and deeds) and photographs that contain or constitute Personal Data.