Policy Ref:	**BI-PL--001**
Issue Number:	**001**
Approved:	August 2018
For Review:	**August 2021**

Information Security and Data Protection Policy

1.0 Introduction

1.1 We hold personally identifiable information (PII) 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 security and data protection and details the measures we have taken to ensure PII 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 carry out our stated objectives
- Accurate and up to date - inaccurate PII 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.

2.0 Objective

2.1 The objective of this policy is to ensure compliance with all relevant data protection and information security legislation including (but not limited to) the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

3.0 Definitions

3.1 **Personally identifiable information (PII):** 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 PII 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.

3.2 **Special category data:** PII 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.

3.3 **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.

3.4 **Record**: Processed data that has been placed into a temporary or physical location, for example, a tenancy agreement, contract of employment or database. A record will contain many different categories or processed data.

3.5 **Data subject**: An identified person, or a person who can be identified (either directly or indirectly) through the application of PII or special category data.

3.6 **Data controller**: The entity that, either alone or jointly with others, determines the purpose, conditions and means of processing PII.

3.7 **Data processor**: The entity that processes PII on behalf of the data controller. We will only use data processors who can provide sufficient guarantees on their data protection practices.

3.8 **Data protection officer (DPO)**: The person who is responsible for making sure that this policy is embedded and applied; the Head of Business Intelligence is our DPO.

3.9 **Data recipient**: The entity to whom PII is disclosed, including any third parties.

3.10 **Processing**: Any operation performed on PII, including (but not limited to) collection, recording, organising, structuring, storage, adaption, retrieval, consultation, use, disclosure, alignment or erasure.

3.11 **Data subject access request (DSAR)**: a right of data subjects to find out what PII 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').

3.11 **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.

3.12 **Data breach**: A breach of security that has resulted in the accidental destruction, loss, alteration, unauthorised disclosure of or access to PII.

3.13 **Profiling**: Any form of automated processing of PII 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.

3.14 **Pseudonymisation**: The processing of PII in such a way that it can no longer be linked to a data subject without the use of additional information, kept separately.

3.15 **Confidential**: Data that we have a legal obligation to keep securely stored, for example employee HR records.

3.16 **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.

3.17 **Unclassified**: Data that is freely available and can be shared with other parties, both internal and external, for example performance scorecards.

4.0 Responsibilities

4.1 The **Head of Business Intelligence** (as the **data protection officer**): is responsible for ensuring that the processing of PII is carried out in accordance with this policy and all applicable legislation. This includes:

- Ensuring systems are adequately protected from unauthorised access and secured against theft and damage to a level that is cost effective
- Ensuring data is accurate and is limited to what we need to deliver our stated priorities
- Maintaining a data retention matrix and making this available to employees
- Maintaining our privacy notice and ensuring that data subjects are made aware of how their PII is being processed
- Ensuring that systems are used for their intended purpose
- Providing appropriate procedures to rectify data breaches or any other notified misuse
- Ensuring data processors understand their responsibilities around information security and data protection
- Co-ordinating our response to DSARs and determining whether requests are 'manifestly excessive'
- Ensuring that breaches of this policy are investigated, the Information Commissioner is notified within 72 hours and data subjects made aware without undue delay
- Validating the effectiveness of our data processing measures
- Co-operating fully with the Information Commissioner on data protection issues.

4.2 **Data processors** are responsible for processing personal data under the instruction of the Data controller and facilitating our response to DSARs within target timescales.

4.3 **Heads of service** and **line managers** are responsible for:

- Monitoring the data retention matrix and advising the data protection officer of any changes to retention dates/timescales

- Collating PII as required so that we can respond to DSARs within target timescales
- Archiving, disposing and/or destroying personal data, both securely and in accordance with the requirements of this policy
- Reporting data breaches to the data protection officer.

4.4 **Employees** are responsible for:

- Reporting data breaches to their line manager/head of service as soon as they become aware of the existence of the breach
- Complying with our privacy notice and developing specific privacy notices wherever new PII is being collected
- Complying with the requirements of this policy.

5.0 Sustainability

5.1 Wherever possible, data will be stored electronically as we increasingly move away from traditional, paper based resources. This policy does, however, apply to PII in all forms, including (but not limited to):

- Paper based materials
- Information stored electronically on information systems, whether deployed or access on or off site
- Information stored on our computer network
- Corporate information stored on any hardware, including mobile devices and removable media, or transmitted by post
- Electronic recording devices, including video, audio and CCTV systems
- Information transmitted via telephone and/or voicemail
- Any other data we own.

6.0 Reporting

6.1 Lawfulness of processing

6.1.1 We will identify our legal bases for processing PII 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 PII 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 PII (particularly where the data subject is a child).

6.1.2 We have embraced privacy by design; before collecting PII 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. We will adopt a risk based approach when implementing technical and organisational measures to protect the rights of data subjects.

6.1.3 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 PII 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.

6.2 Privacy notice

6.2.1 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 PII
c. How PII is managed and when it may be shared with third parties
d. The recipients or categories of recipients of PII (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.

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

- The length of time that PII will be stored, or the criteria used to determine this period
- Whether the provision of PII 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
- The existence of automated decision making, including information on the logic involved and the significance and consequences of such processing (where applicable).

6.3 Data processing

6.3.1 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.

6.3.2 We will only share PII with external organisations if there is a legal obligation for this to be shared 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:

- Password protecting all electronic records that contain PII (if a password needs to be shared this should be sent separately)
- Special category data will only be exchanged through the Criminal Justice Secure email (CJSM) system or similar.
- When exchanging information via email or fax, recipient addresses will be checked carefully prior to transmission
- Using BCC rather than CC when emailing multiple data subjects to avoid sharing email addresses and other PII
- Unsolicited communications requesting information which is not unclassified should not be acted upon until (and unless) the source of the communication has been verified
- 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.

6.3.3 We will work towards a clear desk policy, and employees must ensure that any records containing PII are placed out of sight before leaving their workstation (this includes vehicles). PII must not be stored on general access drives; when stored electronically on team drives records should be password protected to control access.

6.3.4 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: **Bums off seat, Control, Alt, Delete**.

6.3.5 PII that we have collected must not be processed on personally owned devices.

6.3.6 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.

6.3.7 We will work towards classification of 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.

6.3.8 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 PII.

6.3.9 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.

6.4 Data subject access requests (DSAR)

6.4.1 Data subjects can exercise their right to request their PII 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).

6.4.2 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.

6.4.3 Where the data subject makes their request by electronic form, we will respond electronically unless otherwise requested. Where PII 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.

6.5 Data breach reporting

6.5.1 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:

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

6.5.2 We will document all data breaches and report these, together with significant near misses, to our Audit and Risk Committee.

6.5.3 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.

6.6 Data privacy impact assessments (DPIA)

6.6.1 Where we introduce a new policy or initiative 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 description of the processing operation, its purpose and the legal bases for processing
- An risk based assessment of the intended processing
- The measures that will be taken to address risk, including safeguards, security measures and mechanisms to ensure compliance with our legal obligations.

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

7.0 Consultation

7.1 The Beyond Housing Board approved this policy. Future reviews will incorporate consultation with heads of service, senior management, and involved customers.

8.0 Review

8.1 This policy will be reviewed within 12 months of Beyond Housing being in operation and thereafter every two years or wherever changes to legislation impact upon its content (whichever is sooner) by the Head of Business Intelligence.