POLICY: DATA PROTECTION (GDPR)

Sections

1. Purpose and aim of the Policy
2. Important definitions
3. Data protection principles
4. Processing data
5. Collection of data
6. Accuracy of data
7. Timely processing
8. Data security
9. Transferring personal data outside the UK
10. Disclosure and sharing of personal information
11. Dealing with Subject Access Requests
12. Equality impact assessment/Protected characteristics
13. Consultation arrangements

Copies of this Policy are available in alternative formats.

Previous BHSE Policy No:	BM 1.3
Previously agreed and approved by Board:	8 February 2011/10 May 2011/4 November 2015/27 November 2019
Format changes/review (no substantive changes):	10 November 2016/25 May 2018
Agreed and approved by the Board:	30 November 2022
Next review date:	November 2025
Published on website:	Yes

POLICY: DATA PROTECTION (GDPR)

All reference to 'we', 'our' or 'us' in this Policy should be read as meaning Sandbourne Housing Association.

1. Purpose and aim of the Policy

1.1 To set out the principles of Data Protection law and guidance that apply to Sandbourne and how those principles will be applied by us.

1.2 This Policy does not form part of any employee's contract of employment and may be amended at any time. Any breach of this Policy may result in disciplinary action.

1.3 Any questions or concerns about the operation of this Policy should be referred in the first instance to the Data Protection Officer, who is the Head of Housing, or to the employee's line manager.

2. Important definitions

2.1 **Data** is information which is stored electronically, on a computer, or in paper-based filing systems.

2.2 **Data subjects** include all natural individuals about whom we hold personal data.

2.3 **Personal data** means information that relates to an identified, or identifiable, individual. In Sandbourne's case this would include data relating to employees, residents and applicants.

2.4 **Data controller** – an organisation that determines the purpose for the collection and processing of personal data about individuals. Sandbourne is a Data Controller.

2.5 **Data users** include employees and Board members whose work involves using personal data.

2.6 **Data processors** include any person who processes personal data on behalf of a data controller. In Sandbourne's case this will mostly be employees.

2.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

2.8 **Sensitive personal data** includes information about a person's 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 processed under strict conditions, and will usually require the express consent of the person concerned

3. Data protection principles

3.1 Anyone processing personal data must do so in compliance with the seven enforceable principles of good practice. These provide that personal data must be:

3.1.1 processed lawfully, fairly and in a transparent way

3.1.2 processed for relevant and limited purposes and in an appropriate way

3.1.3 adequate, relevant and not excessive for the purpose that it is required

3.1.4 accurate and kept up to date

3.1.5 not kept longer than necessary for the purpose that it is required

3.1.6 collected, processed and stored securely.

3.1.7 The Data Controller is responsible for the data collected, processed and stored on its behalf.

4. Processing data

4.1 Sandbourne has a lawful reason for processing data in relation to its employees, residents who live in its properties and applicants who have applied to live in its properties. This lawful reason applies to before, during and after employment in the case of employees (and applicants for employment) and before, during and after residency in one of Sandbourne's properties for residents (and applicants for residency).

4.2 For personal data to be processed lawfully, the data subject must have consented to the processing, or the processing must be necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. In most cases the data subject's explicit consent to the processing of such data will be required, particularly with regards to the processing of sensitive personal data.

4.3 Data will only be collected, processed and stored for necessary business purposes or where there is a legal obligation on Sandbourne to do so.

4.4 Sandbourne will ensure that data is processed in line with data subjects' rights. Data subjects have a right to:

4.4.1 be kept informed of the data that we hold about them.

4.4.2 access to that data. We will inform data subjects of the procedure for accessing their data.

4.4.3 ask to have inaccurate data amended, completed or removed. We will inform data subjects of our policy on amending personal data.

4.4.4 ask that data is removed when it is no longer required. We will inform data subjects of our policy on destroying personal data.

4.4.5 ask that we restrict the use of their data to that which is absolutely necessary. We will inform data subjects of how we intend to use their data and it will not be used for any other purpose without their express consent, except for circumstances where we are required by law to use or share that data.

4.4.6 object to the use of their personal data in certain circumstances eg direct marketing. With the exception of legal requirements, Sandbourne will always seek the consent of data subjects to use their personal data. This consent will normally be in writing.

5. Collection of data

5.1 Where we collect personal data directly from data subjects, we will inform them about:

5.1.1 The purpose or purposes for which we intend to process that personal data.

5.1.2 The types of third parties, if any, with which we will share or to which we will disclose that personal data.

5.1.3 The means, if any, with which data subjects can limit our use and disclosure of their personal data.

5.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

5.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

6. Accuracy of data

6.1 We will ensure that personal data we hold is accurate and kept up-to-date. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

7. Timely processing

7.1 We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected.

8. Data security

8.1 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.

8.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

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

8.3.1 **Confidentiality** means that only people who are authorised to use the data can access it. This will mainly be employees and Board members and will be limited to those who need the data for their job roles.

8.3.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed. We will aim to update or review personal data at least annually.

8.3.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. We will ensure that data is stored securely and access will only be available to those who need it for their job roles.

8.4 Security procedures include:

8.4.1 **Entry controls.** There is limited access to Sandbourne's offices. Any stranger seen in entry-controlled areas should be reported.

8.4.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind.

8.4.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

8.4.4 **Equipment.** PCs, laptops and phones must be password protected and passwords must be changed regularly. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC, laptop and phone when it is left unattended.

9. Transferring personal data to a country outside the EEA

We will not transfer any personal data we hold to a country outside of the UK, other than as permitted by the Act.

10. Disclosure and sharing of personal information

10.1 We may disclose personal data we hold to third parties:

10.1.1 In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

10.1.2 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.

10.2 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or 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.

10.3 We may also share personal data we hold with selected third parties for the purposes set out in this policy.

11. Dealing with Subject Access Requests

11.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their line manager immediately.

11.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

11.2.1 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

11.2.2 We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

11.3 Our employees will refer a request to their line manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

12. Equality impact assessment/Protected characteristics (as at 30 November 2022 or later amendments/additions)

12.1 Neutral.

13. Consultation arrangements

13.1 Our employees will be consulted on this Policy. Any reasonable suggestions will be taken into account before the Policy is approved by the Board.

Further information:

- Data Protection (GDPR) leaflet
- Data Protection Statement
- Privacy Notice, which includes how we use personal information
- Procedure for access to information
- Protocol for Contacting Residents by Email
- Repairs Text Messaging Service Consent and Preferred Contact Details
- Subject Access Request form (SAR)
- Telephone Call Recording Guidelines

The Guide to the General Data Protection Regulation (GDPR) produced by the Information Commissioner's Office (ICO) is also very useful.