POLICY: DATA PROTECTION (GDPR)

Sections

1. Purpose and aim of the Policy
2. Important definitions
3. Data protection principles
4. Processing data
5. Security
6. Subject access requests
7. Telephone enquiries
8. Equality impact assessment/Protected characteristics
9. 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
Last agreed and approved by the Board:	4 November 2015
Format changes/review (no substantive changes):	10 November 2016/25 May 2018
Agreed and approved by the Board:	27 November 2019
Next review date:	November 2022
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 Before, during, and after employment, we will handle certain personal information in relation to candidates and employees. During the course of our activities, we will collect, store, use and process personal information about our staff in accordance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR).

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 Controller, who is the Chief Executive, 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 data relating to a natural individual who can be identified from that data, or from that data and other information in our possession. It can be factual or it can be an opinion.

2.4 **Data controllers (Sandbourne)** are those who determine the reasons for, and the way in which, any personal data is processed. Sandbourne is the data controller of all personal data used in our business.

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

2.6 **Data processors** include any person who processes personal data on behalf of a data controller.

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 eight enforceable principles of good practice. These provide that personal data must be:

3.1.1 processed fairly and lawfully

3.1.2 processed for limited purposes and in an appropriate way

3.1.3 adequate, relevant and not excessive for the purpose

3.1.4 accurate

3.1.5 not kept longer than necessary for the purpose

3.1.6 processed in line with data subjects' rights

3.1.7 secure

3.1.8 not transferred to people or organisations situated in countries without adequate protection.

4. Processing data

4.1 This will be done fairly and without negatively affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

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 must be processed in line with data subjects' rights. Data subjects have a right to:

4.3.1 request access to any data held about them by a data controller

4.3.2 prevent the processing of their data for direct-marketing purposes

4.3.3 ask to have inaccurate data amended

4.3.4 prevent processing that is likely to cause damage or distress to themselves or anyone else.

5. Notifying data subjects

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

(a) The purpose or purposes for which we intend to process that personal data.

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

(c) 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. Adequate, relevant and non-excessive processing

6.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

7. Accurate data

7.1 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.

8. Timely processing

8.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected.

9. Processing in line with data subject's rights

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

(a) Request access to any data held about them by a data controller.

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended.

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

10. Data security

10.1 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.

10.2 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.

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

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

10.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

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

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

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

11. Transferring personal data to a country outside the EEA

11.1 We will not transfer any personal data we hold to a country outside the European Economic Area (”EEA”), other than as permitted by the Act.

12. Disclosure and sharing of personal information

12.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

12.2 We may also disclose personal data we hold to third parties:

(a) 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.

(b) 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.

12.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, 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.

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

13. Dealing with Subject Access Requests

13.1 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.

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

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

(b) 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.

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

14. Telephone enquiries

14.1 Staff dealing with telephone enquiries should be cautious about disclosing any personal information held by us. They should:

14.1.1 check the caller's identity to make sure that information is only given to a person who is entitled to it

14.1.2 ask that the caller put their request in writing if they do not have proof of the caller's identity

14.1.3 refer the caller to the Chief Executive or their line manager for assistance if they are in any doubt about whether they should disclose information.

15. Equality impact assessment/Protected characteristics (as at 8 January 2019 or later amendments/additions)

15.1 Neutral.

16. Consultation arrangements

16.1 Our staff 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 Statement
- Privacy Notice, which includes how we use personal information
- Procedure for access to information
- Subject Access Request form (SAR)