DATA PROTECTION POLICY

Status: APPROVED

Policy Lead:	Executive Director Business Support
Owned By:	Executive Director Business Support
Date Approved:	Mar-23
Approved By:	BHA Board
Review Date:	Mar-26
Regulatory / Legislative Considerations/ References:	UK General Data Protection Regulation Data Protection Act 2018
Other Documents to be read in conjunction with this policy:	Transparency statements Data Retention Policy Information Security Policy Data Security Breach Management Procedure Response Procedure for Data Subject Requests

Policy Title:	Data Protection Policy
Purpose / Aim of policy:	We process personal data about a number of categories of data subjects, including housing applicants, our customers (and their household members), sharing owners, factored owners, job applicants, current and former colleagues, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members, and members, for a number of specific lawful purposes relevant to our activities and functions as a registered social landlord in Scotland. This Policy sets out how we comply with our data protection obligations and seek to protect personal data that we process as part of our activities and functions as a registered social landlord in Scotland, regardless of the medium on which that personal data is stored. The purpose of this Policy is also to ensure that colleagues understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access during their work with us.
Scope of Policy:	This Policy applies to our processing of personal data of the data subjects listed above.

Definitions:	**criminal records data**	means personal data relating to criminal convictions and offences, allegations, proceedings, and related security measures;
	data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
	data subject	means an individual to whom the personal data relates;
	personal data	means information relating to an individual, who can be identified (directly or indirectly) from that information;
	processing	means obtaining, recording, organising, storing, amending, retrieving, disclosing and / or destroying personal data, or using or doing anything with it; and
	special category data	means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.
Approval Source:	Executive Team	
Equality Impact Assessment:	The application of this policy has due regard for protected characteristics and ensures data subjects are treated fairly	
Sustainability Assessment:	There are no major sustainability implications linked to the contents of this policy	
Partnership Assessment:	There are no partnership implications linked to the contents of this policy.	
Risk Implications:	We take compliance with this Policy very seriously. Failure to comply with the Policy: • puts at risk the data subjects whose personal data is being processed; • carries the risk of significant civil and criminal sanctions for us; and • may, in some circumstances, amount to a criminal offence by a member of our colleagues	

1 Introduction

1.1 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal data and how (and when) we delete that information once it is no longer required.

1.2 We recognise that the correct and lawful treatment of personal data will maintain confidence in our organisation and is conducive to successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we always take seriously. We are exposed to potential fines for failure to comply with the provisions of data protection legislation.

1.3 Our Data Protection Officer (DPO) is responsible for informing and advising us and our staff on our data protection obligations, and for monitoring compliance with those obligations and with our policies. If colleagues have any questions or comments about the content of this Policy or if they need further information, they should contact the DPO. Information on the role and responsibilities of our DPO is contained in Section 16 of this Policy.

1.4 This Policy sets out important information about:

1.4.1 the data protection principles with which we must comply;

1.4.2 what is meant by personal data and special category data;

1.4.3 how we gather, use and (ultimately) delete personal data and special category data in accordance with the data protection principles;

1.4.4 where more detailed privacy information can be found;

1.4.5 data subjects' rights and our obligations in relation to data protection;

1.4.6 the role and responsibilities of our DPO; and

1.4.7 the consequences of failure to comply with this Policy.

2 Data protection principles

2.1 We will comply with the following data protection principles when processing personal data in carrying out our activities and functions:

2.1.1 we will process personal data lawfully, fairly and in a transparent manner;

2.1.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes, unless the processing has been first notified to the data subject;

2.1.3 we will only process personal data that is adequate, relevant and necessary for the above specified, explicit and legitimate purposes;

2.1.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data is deleted or corrected without delay;

2.1.5 we will keep personal data for no longer than is necessary for the purposes for which the personal data is processed; and

2.1.6 we will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

3 Basis for processing personal data and special category data

3.1 In relation to any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

3.1.1 review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing i.e.

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract between us and the data subject;

(c) that the processing is necessary for compliance with a legal obligation to which we are subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another person; or

(e) that the processing is necessary for the purposes of our legitimate interests or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject;

3.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose);

3.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

3.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant transparency statement(s);

3.1.5 where special category data is processed, also identify a lawful special condition for processing that information (see paragraph 3.4.2 below), and document it; and

3.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

3.2 When determining whether our legitimate interests are the most appropriate basis for lawful processing, we will:

3.2.1 conduct a legitimate interests' assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

3.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

3.2.3 keep the LIA under review, and repeat it if circumstances change; and

3.2.4 include information about our legitimate interests in our transparency statement(s).

3.3 Special category data is sometimes referred to as "sensitive personal data".

3.4 We may from time to time need to process special category data as part of our activities and functions as a registered social landlord in Scotland. We will only process special category data if:

3.4.1 we have a lawful basis for doing so as set out in paragraph 3.1.1 above; and

3.4.2 one of the special conditions for processing special category data applies e.g.

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights of the data subject or our employment law obligations;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which is manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

3.5 Before processing any new categories of special category data, staff must notify the DPO of the proposed processing, in order that the DPO may assess whether one of the above special conditions applies.

3.6 New categories of special category data will not be processed until:

3.6.1 the assessment referred to in paragraph 5.5 above has taken place; and

3.6.2 the data subject has been properly informed (by way of transparency statement) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

3.7 We do not carry out automated or electronic decision-making (including profiling) based on a data subject's special category data.

3.8 Our transparency statements set out the types of special category data that we process, what it is used for and the lawful basis for the processing.

3.9 Consent is one of the lawful bases for processing personal data and special category data.

3.10 A data subject consents to processing of their personal data if they indicate agreement either by a statement or positive action to the processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be enough. If consent is given in a document which deals with other matters, then consent must be kept separate from those other matters. An example of this is in our transparency statements where the consent section is in red text and is separated from the other text within a box.

3.11 Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is to be processed for a different and incompatible purpose which

was not disclosed when the data subject first consented via the relevant transparency statements.

4 DPIAs

4.1 Where processing of personal data is likely to result in a high risk to a data subject's data protection rights (e.g., where we are planning to use a new form of technology which involves or could involve the processing of personal data, such as a new document management system, colleague monitoring or drones for roof condition surveys), we will, before commencing the processing, carry out a DPIA to assess:

4.1.1 whether the processing is necessary and proportionate in relation to its purpose;

4.1.2 the risks to data subjects; and

4.1.3 what measures can be put in place to address those risks and protect personal data.

4.2 Before any new form of technology is introduced, colleagues must contact the DPO in order that a DPIA can be carried out.

4.3 If the technology involves the processing of employee personal data, the DPO will seek the views of a representative group of colleagues as part of undertaking the DPIA.

5 Documentation and records

5.1 We will keep written records of our processing activities, including:

5.1.1 our name and contact details, including the contact details of the DPO;

5.1.2 the purposes of processing personal data;

5.1.3 a description of the categories of data subjects and categories of personal data processed by us;

5.1.4 categories of recipients of personal data processed by us;

5.1.5 where relevant, details of regulated transfers of personal data to countries outside the UK, including documentation associated with how we protect the personal data after transfer;

5.1.6 how long we keep personal data; and

5.1.7 a description of the technical and organisational security measures that we have in place to protect the security of personal data.

5.2 As part of our record of processing activities, we document:

5.2.1 information required for our transparency statements;

5.2.2 records of consent (which may be in writing, contained within our transparency statements or otherwise recorded);

5.2.3 controller-processor (service provider) contracts;

5.2.4 the location of personal data within our systems;

5.2.5 DPIAs; and

5.2.6 records of data breaches.

5.3 If we process special category data or criminal records data, we will keep written records of:

5.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

5.3.2 the legal basis for our processing; and

5.3.3 whether we retain and erase the personal data in accordance with our Data Retention Procedure and, if not, the reasons for not following the procedure.

5.4 We will conduct regular audits of the personal data that we process and update our documentation, accordingly, including by:

5.4.1 distributing questionnaires and interviewing colleagues to obtain to a complete picture of our processing activities; and

5.4.2 reviewing our policies, procedures, contracts and agreements to address areas, such as retention, security and data sharing.

5.5 We document our processing activities in electronic form, so we can add, remove and amend information easily.

6 Transparency statements

6.1 We will issue transparency statements from time to time, informing data subjects about the personal data that we process about them, how they can expect their personal data to be used and for what purposes. This applies whether we collect personal data directly from the data subject or from third parties.

6.2 We will take appropriate measures to provide information in transparency statements in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

7 Data subjects' rights and requests

7.1 Data subjects have rights when it comes to how we process their personal data. These include rights to:

7.1.1 withdraw consent to processing of their personal data at any time;

7.1.2 receive certain information about our personal data processing activities;

7.1.3 request access to their personal data that we process about them;

7.1.4 ask us to erase their personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate personal data or to complete incomplete personal data;

7.1.5 restrict processing of personal data in specific circumstances;

7.1.6 challenge processing which has been justified based on our legitimate interests or in the public interest;

7.1.7 request a copy of an agreement under which personal data is transferred by us to another organisation based outside of the UK;

7.1.8 prevent processing of personal data that is likely to cause damage or distress to the data subject or anyone else;

7.1.9 be notified of a data breach which is likely to result in high risk to their rights and freedoms;

7.1.10 make a complaint to the Information Commissioner's Office about our processing of their personal data; and

7.1.11 in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

7.2 The identity of the data subject exercising any of the rights listed above must be verified.

7.3 Colleague must immediately forward any such request received by them to the DPO.

7.4 The procedures for handling and responding to data subjects' rights requests are contained within our Response Procedures for Data Subject Requests.

8 Staff obligations

8.1 Colleagues are responsible for keeping their personal data up to date. Colleagues should let the People and Culture Specialist know if the information they have provided to us changes, for example, if they move to a new house.

8.2 Colleagues may have access to a range of personal data during their employment and colleagues must help us to meet our data protection obligations.

8.3 If staff have access to personal data, they must:

8.3.1 only access the personal data that they have authority to access, and only for authorised purposes;

8.3.2 only allow other colleagues to access personal data if they have appropriate authorisation;

8.3.3 only allow third parties to access personal data if they have specific authority to do so from the DPO or their line manager;

8.3.4 ensure that any sharing of personal data complies with the transparency statement provided to data subjects and the third party with whom it is shared agrees to put appropriate security measures in place to protect the personal data;

8.3.5 keep personal data secure (e.g., by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other appropriate precautions);

8.3.6 not remove personal data, or devices containing personal data (or which can be used to access it), from our premises, unless appropriate security measures are in place (such as encryption or password protection) to secure the information and the device; and

8.3.7 not store personal data on local drives or on personal devices that are used for work purposes.

8.4 Colleagues should contact the DPO if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

8.4.1 processing of personal data without a lawful basis for its processing or, in the case of special category data, without one of the conditions in paragraph 3.4.2 being met;

8.4.2 any data breach as set out in paragraph 11.1 below;

8.4.3 access to personal data without the proper authorisation;

8.4.4 personal data not kept or deleted securely;

8.4.5 removal of personal data, or devices containing personal data (or which can be used to access it), from our premises without appropriate security measures being in place; or

8.4.6 any other breach of this Policy or of any of the data protection principles set out in paragraph 2.1 above.

9 Information security

9.1 We will use appropriate technical and organisational measures (based on our size, available resources, volume of personal data processed and risks) to keep personal data secure, and to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These may include:

9.1.1 making sure that, where possible, personal data is encrypted, or password protected;

9.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Confidentiality means only those who need to know and are authorised to use personal data can access it. Integrity means that the personal data is accurate and suitable for the purpose for which it is processed. Availability means that authorised users can access the personal data when they need it for authorised purposes;

9.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and

9.1.4 a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

9.2 Where we use external organisations to process our personal data on our behalf, such as our contractors and service providers, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security our of personal data. Contracts with external organisations must provide that:

9.2.1 the organisation may act only on our written instructions;

9.2.2 colleagues of the organisation processing the personal data are subject to a duty of confidence;

9.2.3 appropriate measures are taken to ensure the security of processing;

9.2.4 sub-contractors are only engaged by the organisation with our prior consent and under a written contract;

9.2.5 the organisation will assist us in providing subject access and allowing data subjects to exercise their data protection rights;

9.2.6 the organisation will assist us in meeting our obligations in relation to the security of processing, the notification of data breaches and DPIAs;

9.2.7 the organisation will delete or return all personal data to us as requested at the end of the contract; and

9.2.8 the organisation will submit to audits and inspections, provide us with whatever information we need to ensure that they are meeting their data protection obligations, and tell us immediately if the organisation is asked to do something that could breach data protection law.

9.3 Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is amended, colleagues must seek approval of its terms by the DPO.

9.4 Further information is contained in our Information Security Policy.

10 Storage and retention of personal data

10.1 Personal data will be kept securely.

10.2 Personal data should not be retained for longer than necessary. The length of time over which personal data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. Colleagues should follow our Data Retention Procedure, which sets out the relevant retention period. Where there is any uncertainty, colleagues should consult the DPO.

10.3 Personal data that is no longer required will be deleted permanently from our systems and any hard copies will be destroyed securely.

11 Data breaches

11.1 A data breach may take many different forms, for example:

11.1.1 loss or theft of information or equipment on which personal data is stored;

11.1.2 unauthorised access to or use of personal data either by a colleague or third party;

11.1.3 loss of personal data resulting from an equipment or systems (including hardware and software) failure;

11.1.4 human error, such as accidental deletion or alteration of personal data;

11.1.5 unforeseen circumstances, such as a fire or flood;

11.1.6 deliberate attacks on our IT systems, such as hacking, viruses, or phishing scams; and

11.1.7 “blagging” offences, where personal data is obtained by deceiving our organisation.

11.2 We will:

11.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible, within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of data subjects; and

11.2.2 notify the affected data subjects if a data breach is likely to result in a high risk to their rights and freedoms and where notification is required by law.

11.2.3 The DPO must be notified immediately as soon as staff become aware of a data breach. Colleagues should not attempt to investigate the matter themselves.

12 Transfers of personal data outside the UK

We may only transfer personal data outside the UK on the basis that that recipient country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards so far as data protection is concerned. Further advice must be obtained from the DPO.

13 Training

We will ensure that colleagues are adequately trained regarding their data protection responsibilities. Colleagues whose roles require regular access to personal data will receive additional training to help them understand their duties and how to comply with them.

14 Role and responsibilities of the DPO

14.1 Data protection legislation states that our DPO must have professional and expert knowledge of data protection law and carry out the following responsibilities:

14.1.1 inform and advise the organisation on data protection legislation requirements;

14.1.2 monitor and audit our compliance with data protection law and our data protection policies;

14.1.3 deliver data protection training to all colleagues and raise awareness of data protection;

14.1.4 complete DPIAs; and

14.1.5 liaise and co-operate with the Information Commissioner's Office and data subjects on our behalf.

14.2 In addition to the above, our DPO will also assist in carrying out the following:

14.2.1 completing data mapping exercises, which set out what personal data the organisation processes, who it is about, the purposes for which it is processed, and who it is shared with;

14.2.2 determining our lawful basis (or bases) for processing personal data and the special conditions for processing special category data;

14.2.3 assisting us in maintaining written records and documentation regarding our processing activities;

14.2.4 managing and responding to data security incidents and breaches in accordance with the Data Security Breach Management Procedure;

14.2.5 preparing appropriate contracts for us to enter into with external organisations who process personal data on our behalf, data sharing agreements and other commercial agreements;

14.2.6 developing and managing our data protection strategy;

14.2.7 handling and resolving complaints from aggrieved data subjects;

14.2.8 "horizon scanning" for data protection law that could affect our activities and functions as a registered social landlord in Scotland; and

14.2.9 promoting and embedding a culture of data protection compliance in the organisation in all respects.

15 Consequences of failure to comply

15.1 Due to the importance of this Policy, failure to comply with any requirement of it may lead to disciplinary action for a member of staff under our procedures, and this action may result in dismissal for gross misconduct. If an external organisation breaches this Policy, they may have their contract terminated by us with immediate effect.

15.2 Any questions or concerns about this Policy should be directed to the DPO.

16 Review and updates to this Policy

We will review and update this Policy in accordance with our data protection obligations and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.