Data Protection Policy

C.04 V.6 – November 2021

Policy Number	**C.04**			
Document Owner	**Corporate**			
Review Frequency	**3 yearly**			
Reviewed by	**Information Law Solutions**			
First Approved	**November 2001**			
Last Reviewed	**November 2021**			
Next Review Due	**November 2024**			
Version Number	**6**			
Consultation Required	**Yes**		**No**	**x**
Equalities Impact Assessment	**Yes**		**No**	**x**
Added to Website	**Yes**	**x**	**No**	

SSHC Reference	
SHR Reference	

Related Documents

- C.02 Information Security Policy
- C.10 Publication Scheme – guide to information
- C.17 Notifiable Events Policy
- C.20 Access to Information Policy
- C.22 Data Retention and Destruction Policy
- CP.03 Data Breach Management Procedures
- CP.02 Responding to Subject Access Request Procedures
- CP.04 Notifiable Events Procedure
- CP.06 Access to Information Procedure

Translation Statement

We can give you this document in another way . Please tell us what you need. Contact us if you need help

Compliance

This policy has been drafted to ensure that it complies with current legislation and industry good practice.

Equality & Diversity

Fyne Homes is committed to providing services which embrace diversity and which promote equality of opportunity. As an employer we are also committed to equality and diversity within our workforce. Our goal is to ensure that these commitments, reinforced by our Values, are embedded in our day-to-day working practices.

Openness & Confidentiality

Fyne Homes believes that its members, tenants and other interested parties should have access to information on how it conducts itself. This means that unless information requested is considered commercially sensitive or personally confidential it will be made available on request.

Data Protection

Fyne Homes recognises the importance of data protection legislation, including the General Data Protection Regulation, in protecting the rights of individuals in relation to personal information that we may handle and use about them, whether on computer or in paper format. We will ensure that our practices in the handling and use of personal information during the processes and procedures outlined in this policy comply fully with data protection legislation. More information is available from our Data Protection Officer.

1 Introduction

This Policy sets out important information about:

- the data protection principles with which we, Fyne Homes, must comply;
- what is meant by personal information and sensitive personal information;
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found;
- rights and our obligations in relation to data protection; and
- the consequences of failure to comply with this Policy.

1.1 We process personal information about a number of categories of data subjects, including housing applicants, our tenants (and their household members), sharing owners, factored owners, job applicants, current and former employees, suppliers, contractors, business contacts (including at other registered social landlords, regulators, local authorities and other agencies), committee members and members for a number of specific lawful purposes relevant to our activities and functions as a registered social landlord in Scotland.

1.2 This Policy sets out how we comply with our data protection obligations and seek to protect personal information 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 information is stored. The purpose of the Policy is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access during their work with us.

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

1.4 We recognise that the correct and lawful treatment of personal information will maintain confidence in our organisation and is conducive to successful business operations. Protecting the confidentiality and integrity of personal information is a critical responsibility that we always take seriously. We are exposed to potential fines of up to £17.5 million or 4% of our total annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of data protection legislation.

1.5 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 members of staff 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 the DPO is contained in Section 16 of this Policy.

2 Scope

2.1 This Policy applies to our processing of personal information of data subjects listed in paragraph 1.1.

2.2 Staff should refer to our transparency statements and our other relevant policies and procedures, including the Information Security Policy, the Data Security Breach Management Procedure, and Response Procedures for Data Subject Requests, which contain further information regarding the protection of personal information.

3 Definitions

For the purposes of this Policy:

criminal records information	means personal information 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 information;
data subject	means an individual to whom the personal information relates;
personal information	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 information, or using or doing anything with it; and
sensitive personal information	means personal information 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.

4 Data protection principles

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

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information 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;

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

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

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

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

5 Basis for processing personal information and sensitive personal information

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

5.1.1 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;

5.1.2 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);

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

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

5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 5.4.2 below), and document it; and

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

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

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

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

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

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

5.3 Sensitive personal information is sometimes referred to as "special categories of personal information".

5.4 We may from time to time need to process sensitive personal information as part of our activities and functions as a registered social landlord in Scotland. We will only process sensitive personal information if:

5.4.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above; and

5.4.2 one of the special conditions for processing sensitive personal information 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 information 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.

5.5 Before processing any new categories of sensitive personal information, staff must notify the DPO of the proposed processing, in order that the DPO may assess whether one of the above special conditions applies.

5.6 Sensitive personal information will not be processed until:

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

5.6.2 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.

5.7 We do not carry out automated or electronic decision-making (including profiling) based on a data subject's sensitive personal information.

5.8 Our transparency statements set out the types of sensitive personal information that we process, what it is used for and the lawful basis for the processing.

5.9 Consent is one of the lawful bases for processing personal information and sensitive personal information.

5.10 A data subject consents to processing of their personal information 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 separated from the other text within a box.

5.11 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 information 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.

6 DPIAs

6.1 Where processing 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 information, such as a new document management system, employee monitoring or drones for roof condition surveys), we will, before commencing the processing, carry out a DPIA to assess:

6.1.1 whether the processing is necessary and proportionate in relation to its purpose;
6.1.2 the risks to data subjects; and
6.1.3 what measures can be put in place to address those risks and protect personal information.

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

6.3 If the technology involves the processing of employee personal information, the DPO will seek the views of a representative group of employees as part of undertaking the DPIA.

7 Documentation and records

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

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

7.1.2 the purposes of processing personal information;

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

7.1.4 categories of recipients of personal information processed by us;
where relevant, details of regulated transfers of personal information to countries outside the United Kingdom (UK), including documentation associated with how we protect the personal information after transfer;
how long we keep personal information; and

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

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

7.2.1 information required for our transparency statements;

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

7.2.3 controller-processor (service provider) contracts;

7.2.4 the location of personal information within our systems;

7.2.5 DPIAs; and

7.2.6 records of data breaches.

7.3 If we process sensitive personal information or criminal records information, we will keep written records of:

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

7.3.2 the legal basis for our processing; and

7.3.3 whether we retain and erase the personal information in accordance with our Data Retention Policy and, if not, the reasons for not following the policy.

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

7.4.1 distributing questionnaires and interviewing staff to obtain to a complete picture of our processing activities; and

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

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

8 Transparency statements

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

8.2 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.

9 Data subjects' rights and requests

9.1 Data subjects have rights when it comes to how we process their personal information.

9.2 We will handle rights requests in accordance with our Response Procedures for Data Subject Requests.

10 Staff obligations

10.1 Staff are responsible for keeping their personal information up to date. Staff should let the Human Resources department know if the information they have provided to us changes, for example, if they move to a new house.

10.2 Staff may have access to a range of personal information during their employment and staff must help us to meet our data protection obligations.

10.3 If staff have access to personal information, they must:

10.3.1 only access the personal information that they have authority to access, and only for authorised purposes

10.3.2 only allow other staff to access personal information if they have appropriate authorisation;

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

10.3.4 ensure that any sharing of personal information 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 information;

10.3.5 keep personal information secure by complying with our Information Security Policy; and

10.3.6 not store personal information on local drives or on personal devices that are used for work purposes.

10.4 Staff 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):

10.4.1 processing of personal information without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 5.4.2 being met;

10.4.2 access to personal information without the proper authorisation; or

10.4.3 any other breach of this Policy or of any of the data protection principles set out in paragraph 4.1 above.

11 Information security

11.1 We will keep personal information secure in accordance with our Information Security Policy.

11.2 Where we use external organisations to process our personal information on our behalf, such as our contractors and service providers, our contracts with them must provide that:

11.2.1 the organisation may act only on our written instructions;

11.2.2 employees of the organisation processing the personal information are subject to a duty of confidence;

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

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

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

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

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

11.2.8 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.

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

12 Storage and retention of personal information

12.1 We will comply with our Data Retention Policy, which sets out the length of time for which we will store and retain personal information.

13 Data breaches

13.1 We will manage and record actual or suspected personal data breaches in accordance with our Data Breach Management Procedure.

14 Transfers of personal information outside the UK

14.1 We may only transfer personal information 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.

15 Training

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

15.2 The DPO will deliver annual or more frequent staff refresher training to ensure that staff are aware of their data protection responsibilities on an ongoing basis or in response to any changes in data protection law or best practice, respectively.

16 Role and responsibilities of the DPO

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

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

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

16.1.3 deliver data protection training to all staff and raise awareness of data protection;

16.1.4 complete DPIAs; and

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

16.2 In addition to the above, our DPO will also carry out the following responsibilities:

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

16.2.2 determine our lawful basis (or bases) for processing personal information and the special conditions for processing sensitive personal information;

16.2.3 assist us in maintaining written records and documentation regarding our processing activities;

16.2.4 manage and respond to data security breach incidents in accordance with the Data Security Breach Management Procedure;

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

16.2.6 develop and manage our data protection strategy;

16.2.7 handle and resolve complaints from aggrieved data subjects;

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

16.2.9 promote and embed a culture of data protection compliance in the organisation in all respects.

17 Consequences of failure to comply

17.1 We take compliance with this Policy very seriously. Failure to comply with the Policy:

17.1.1 puts at risk the data subjects whose personal information is being processed;

17.1.2 carries the risk of significant civil and criminal sanctions for us; and

17.1.3 may, in some circumstances, amount to a criminal offence by a member of our staff.

17.2 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.

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

17. Reviewing Process

17.1 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.

17.2 If there is a procedural delay in the policy revision then the relative legislation in force at the time will prevail.

Version number	Revision Date	Part of doc revised	Reason for revision	Approved by
5	17.4.19	All	Fully revised in line with new GDPR regulations	Mgt Comm
6	24.1121	References to the EU updated to the UK throughout to reflect post Brexit changes to data protection law.	Brexit and general best practice.	

		New Section 16 on the role and responsibilities of the DPO.		