DATA PROTECTION HANDBOOK

Implemented	October 2018
Reviewed On	March 2023
Next Review Due	March 2026

Contents

1. INTRODUCTION

1.1 The purpose of this handbook is to provide a framework for West of Scotland Housing Association (WSHA) to comply with data protection legislation and to ensure that all obtaining and processing of personal data is carried out in with relevant legislation and regulations.

1.2 This handbook contains the policies required by WSHA and describes how WSHA manages personal data. The handbook also contains relevant documentation and templates and used and information on external sources of information.

1.3 This handbook sets out how we will manage personal data in the Association, ensuring compliance with legislation and it establishes an overall framework for that consists of the following:

Document	Purpose
Data Protection Policy	This policy document outlines how the Association complies with the data protection principles; how we gather, use and delete personal information and our rights and obligations in relation to data protection.
Information Security Policy	The purpose of this policy is to protect against potential breaches of confidentiality; ensure all our information assets and IT facilities are protected against damage, loss or misuse.
Data Breach Management Policy	This policy document places obligations on staff to report actual or suspected data breaches; and sets out our procedure for managing and recording actual or suspected personal data breaches.
Response Procedures for Data Subject Access Requests	These procedures outline the steps to follow to handle and respond to a Data Subject Access Request.
Data Retention Policy	This document outlines the Association's policy in relation to the retention of data. It sets out clear guidelines on the length of time data should be retained.

1.4 In addition to the above policies, we will ensure all operational policies contain a Data Protection Statement where relevant e.g. Allocations, Anti Social Behaviour. We will also ensure that Data Protection is considered in all aspects of decision making.

Relevant Legislation

The Association has to comply with the following:

- **UK General Data Protection Regulation**
- **Data Protection Act 2018**

2. ROLES AND RESPONSIBILITIES

Corporate Management Team

- Ensure effective implementation of this handbook
- Ensure staff are aware of the handbook
- Ensure data processing is in line with the policies detailed in this handbook
- Ensure data breaches are dealt with accordingly
- Ensure data protection is considered as part of all decision making
- Ensure compliance with legislation
- Ensure relevant training is in place for staff and the Board

Data Protection Officer (Corporate Services Manager)

- To inform and advise about our obligations to comply with the UK GDPR and other data protection laws
- To monitor compliance with the UK GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and the Board and conducting internal audits
- To advise on, and to monitor, data protection impact assessments
- To cooperate with the Information Commissioner; and to be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc)
- When carrying out their tasks the DPO is required to take into account the risk associated with the processing we are undertaking. They must have regard to the nature, scope, context and purposes of the processing
- The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to our organisation

Managers

- Comply with the Association's Data Protection Policies and Procedures contained in this handbook

- Ensure all staff are aware of and comply with the policy and procedures
- Ensure all data processing in your section is carried out in line with the Association's Data Protection Policies and Procedures

All Staff

- Comply with the policies and procedures contained in this handbook

3. DATA PROTECTION POLICY

DATA PROTECTION POLICY

This Policy sets out important information about:

- the data protection principles with which we, West of Scotland HA, 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 Introduction

1.1 We obtain, keep and use personal information about housing applicants, our tenants (and their household members), factored owners, job applicants, current and former employees, contractors, business contacts, 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.

1.2 This Policy sets out how we comply with our data protection obligations and seek to protect personal information that we handle and use 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 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 our DPO is contained in Section 16 of this Policy.

2 Scope

2.1 This Policy applies to the personal information of housing applicants, our tenants (and their household members), factored owners, job applicants, current and former employees, contractors, business contacts, apprentices, committee members and members.

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

2.3 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.

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 New categories of 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 coloured text and is 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;

7.1.5 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;

7.1.6 how long we keep personal information; and

7.1.7 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 collect and hold 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 handle their personal information. These include rights to:

9.1.1 withdraw consent to processing of their personal information at any time;

9.1.2 receive certain information about our personal information processing activities;

9.1.3 request access to their personal information that we hold about them;

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

9.1.5 restrict processing of personal information in specific circumstances;

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

9.1.7 request a copy of an agreement under which personal information is transferred by us to another organisation based outside of the EEA;

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

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

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

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

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

9.3 Staff must immediately forward any such request received by them to the DPO.

9.4 The procedures for handling and responding to data subjects' rights requests are contained within 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 (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other appropriate precautions);

10.3.6 not remove personal information, or devices containing personal information (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

10.3.7 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 any data breach as set out in paragraph 13.1 below;

10.4.3 access to personal information without the proper authorisation;

10.4.4 personal information not kept or deleted securely;

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

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

11.1.1 making sure that, where possible, personal information is encrypted;

11.1.2 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 information can access it. Integrity means that the personal information is accurate and suitable for the purpose for which it is processed. Availability means that authorised users can access the personal information when they need it for authorised purposes;

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

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

11.2 Where we use external organisations to process our personal information 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 information. Contracts with external organisations 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.

11.4 Further information is contained in our Information Security Policy.

12 Storage and retention of personal information

12.1 Personal information will be kept securely.

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

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

13 Data breaches

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

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

13.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

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

13.1.4 human error, such as accidental deletion or alteration of personal information;

13.1.5 unforeseen circumstances, such as a fire or flood;

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

13.1.7 “blagging” offences, where personal information is obtained by deceiving our organisation.

13.2 We will:

13.2.1 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

13.2.2 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.

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

14 Transfers of personal information outside the UK

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

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.

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 assist in carrying out the following:

16.2.1 completing 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 determining our lawful basis (or bases) for processing personal information and the special conditions for handling and using sensitive personal information;

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

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

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

16.2.6 developing and managing our data protection strategy;

16.2.7 handling and resolving complaints from aggrieved data subjects;

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

16.2.9 promoting and embedding 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.

4. INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

1 Introduction

1.1 We, West of Scotland HA, are committed to the highest standards of information security.

1.2 Data protection legislation requires us to:

1.2.1 use technical and organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal information;

1.2.2 implement appropriate technical and organisational measures to demonstrate that we have considered and integrated data protection compliance measures into our personal information processing activities; and

1.2.3 demonstrate that we have used or implemented such measures.

1.3 The purpose of this Policy is to:

1.3.1 protect against potential breaches of confidentiality;

1.3.2 ensure all our information assets and IT facilities are protected against damage, loss or misuse;

1.3.3 supplement our Data Protection Policy to ensure that all staff are aware of and comply with data protection legislation as part of their roles at our organisation; and

1.3.4 increase awareness and understanding within the organisation of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the personal information that they handle and use as part of their roles.

1.4 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.

2 Definitions

For the purposes of this Policy:

business information	means business-related information, other than personal information relating to housing applicants, tenants (and their household members), sharing owners, factored owners, job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members and members;
confidential information	means trade secrets or other confidential information (either belonging to us or to third parties);
personal information	means information relating to an individual who can be identified (directly or indirectly) from that information; 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), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3 Roles and responsibilities

3.1 Information security is the responsibility of all our staff. Our Data Protection Officer (DPO) is responsible for:

3.1.1 monitoring and implementing this Policy;

3.1.2 monitoring potential and actual security breaches;

3.1.3 ensuring that staff are aware of their responsibilities through training and issuing guidance and communications to them; and

3.1.4 ensuring compliance with data protection legislation and guidance issued by the Information Commissioner's Office.

4 Scope

4.1 The information covered by this Policy includes all written, spoken and electronic information held, used or transmitted by or on our behalf, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

4.2 This Policy applies to all staff, including employees and apprentices.

4.3 All staff must be familiar with this Policy and comply with its terms when undertaking their roles with the organisation.

4.4 Information covered by this Policy may include:

4.4.1 personal information relating to housing applicants, tenants (and their household members), sharing owners, factored owners, job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members and members;

4.4.2 other business information; and

4.4.3 confidential information.

4.5 This Policy supplements our Data Protection Policy and other relevant policies (including the Data Breach Management Policy) and transparency statements, and the contents of those policies and statements must be considered, as well as this Policy.

4.6 We will review and update this Policy in accordance with our data protection and other obligations and we may amend, update or supplement it from time to time.

5 General principles

5.1 All our information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

5.2 Personal information must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

5.3 Staff should discuss with the DPO the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information that they access as part of their roles at the organisation.

5.4 Our information is owned by the organisation and not by any individual or department within the organisation. Our information must be used only in connection with work being carried out for the organisation and not for other commercial or personal purpose.

5.5 Personal information must be used only for the specified, explicit and legitimate purposes for which it was collected in accordance with data protection legislation.

6 Information management

6.1 Personal information must be processed in accordance with:

6.1.1 the data protection principles, set out in our Data protection Policy; and

6.1.2 all other relevant policies.

6.2 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.

6.3 Personal information and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with our Data Retention Policy.

7 Human Resources information

7.1 Given the internal confidentiality of personnel files, access to such information is limited to the Human Resources department. Other staff are not authorised to access that information (although line managers may have access for recruitment and disciplinary matters).

7.2 Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

7.3 Staff may ask to see their personnel files and any other personal information in accordance with their rights under data protection legislation. Further information is available in our Response Procedures for Data Subject Requests and from our DPO.

8 Access to offices and information

8.1 Office doors and keys and access codes must always be kept secure and keys and access codes must not be given to any third party at any time.

8.2 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by e.g. through ground floor windows. If this cannot be avoided, then blinds should always be positioned to prevent this.

8.3 Visitors must be required to sign in at reception, always accompanied and never left alone in areas where they could have access to confidential information.

8.4 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains our information, then steps should be taken to ensure that no confidential information is visible.

8.5 Whenever possible, at the end of each day, or when desks are unoccupied, all paper documents and devices containing confidential information must be securely locked away.

9 Computers and IT

9.1 Password protection and encryption must be used, where available, on our systems to maintain confidentiality.

9.2 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down in places where they are visible or shared with others.

9.3 Computers and other electronic devices must be locked when not in use and when staff leave their desks, to minimise the risk of accidental loss or disclosure.

9.4 Confidential information must not be copied onto portable media without the express authorisation of the IT department and must be encrypted. Information held on any of these devices should be transferred to our document management system as soon as possible for it to be backed up and then deleted from the device.

9.5 Staff must ensure they do not introduce viruses or malicious code on to our systems. Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact the IT department for authorisation and guidance on appropriate steps to be taken to ensure compliance.

10 Disposal of computers and IT equipment

10.1 IT equipment (which includes its storage media) will be disposed of at the end of its useful life. Such equipment may store business information, confidential information and personal information and must therefore be disposed of in a secure manner to protect such information and to ensure that it cannot be accessed post disposal.

10.2 Prior to disposal, consideration should be given to whether it is possible to re-use IT equipment within the organisation, wherever possible.

10.3 If re-use is not possible, then the IT equipment must be disposed of via our contractor, who will remove the IT equipment from our office and issue a certificate to us to confirm that it has been disposed of securely and that all storage media have been wiped and destroyed. Secure disposal means that the IT equipment is destroyed in a manner that maintains the security of the IT equipment up to the point of destruction. We will only use contractors who provide sufficient guarantees in these regards.

10.4 Staff must not attempt to wipe storage media themselves, as deleting a file does not permanently delete it and put it beyond use.

10.5 If staff have access to the organisation's IT equipment at home or use portable devices as part of their roles, then such IT equipment must be returned to the

organisation for disposal and must not be retained by staff or otherwise disposed of in domestic recycling or dump facilities.

10.6 The organisation will maintain an IT equipment destruction register, recording details of the IT equipment that has been disposed of by the organisation (including the IT equipment's asset number) and the method of destruction), together with copies of the certificates issued by our contractor under paragraph 10.3.

11 Communications and transfer of information

11.1 Staff must be careful about maintaining confidentiality when speaking in public places e.g. when speaking in the front office area or outwith the office either in person or via telephone.

11.2 Confidential information must be marked "confidential" and circulated only to those who need to know the information during their work for the organisation.

11.3 Confidential information must not be removed from our offices, unless required for authorised business purposes, and then only in accordance with paragraph 11.4 below.

11.4 Where confidential information is permitted to be removed from our offices, all reasonable steps must be taken to ensure that the integrity and confidentiality of the information are maintained. Staff must ensure that confidential information is:

11.4.1 stored on an encrypted device, which has been authorised by the IT department, with strong password protection, and which is kept locked when not in use;

11.4.2 when in paper format, not transported in clear or other unsecured bags or cases;

11.4.3 not read in public places (e.g. waiting rooms, cafes and on public transport); and

11.4.4 not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots and cafes).

11.5 Postal and e-mail addresses and telephone numbers should be checked and verified before information is sent to them. Care should be taken with e-mail addresses to ensure that Microsoft Outlook auto-complete features have not inserted incorrect addresses.

11.6 All sensitive or particularly confidential information should be encrypted or password protected before being sent by e-mail or be sent by recorded delivery and its delivery tracked.

12 Personal e-mail and cloud storage accounts

12.1 Personal e-mail accounts, such as Yahoo, Google or Hotmail and cloud storage services, such as Dropbox, iCloud and OneDrive, are vulnerable to hacking. They

do not provide the same level of security as the services provided by our own IT systems.

12.2 Staff must not use a personal e-mail account or cloud storage account for our business purposes.

12.3 If staff need to transfer a large amount of personal information, they should contact the IT department for assistance.

13 Home working

13.1 Staff must not take our information home unless required for authorised business purposes, and then only in accordance with paragraph 13.2 below.

13.2 Where staff are permitted to take our information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

13.2.1 personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by household members or visitors; and

13.2.2 all personal and confidential information must be returned to and disposed of at the office and not in domestic waste or at public recycling facilities.

13.3 Staff must not store confidential information on their home computers and devices.

14 Transfer to third parties

14.1 Third parties should be used to process our information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be "processors" for the purposes of data protection legislation. Examples of processers include our contractors, consultants and professional advisers.

14.2 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the DPO for more information.

15 Training

15.1 All staff will receive training on information security and confidentiality. New staff will receive training as part of the induction process. Further training will be provided on a regular basis or whenever there is a substantial change in the law or our policy and procedure.

15.2 Training is provided by the DPO and attendance is compulsory for all staff at all levels.

16 Reporting breaches

16.1 All members of staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows us to:

16.1.1 investigate the failure and take remedial steps, if necessary;

16.1.2 maintain a register of compliance failures; and

16.1.3 make any applicable notifications to the Information Commissioner's Office, the Scottish Housing Regulator and affected data subjects, if necessary.

16.2 Reference should be made to our Data Breach Management Policy for our reporting procedure.

17 Consequences of failure to comply with this Policy

17.1 We take compliance with this Policy very seriously. Failure to comply with it puts us at significant risk.

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.

Last updated: January 2023

5. DATA BREACH MANAGEMENT POLICY

DATA BREACH MANAGEMENT POLICY

1 Introduction

1.1 This Policy:

1.1.1 places obligations on staff to report actual or suspected personal data breaches; and

1.1.2 sets out our procedure for managing and recording actual or suspected personal data breaches.

1.2 This Policy applies to all staff, and to all personal information and sensitive personal information held by us. This Policy supplements our Data Protection Policy and Information Security Policy.

1.3 We, West of Scotland HA, 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.

1.4 Definitions:

For the purposes of this Policy:

Data Breach Team	means the members of staff at the organisation responsible for investigating personal data breaches;
data subject	means an individual to whom the personal information relates;
personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed;

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), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

2 Responsibility

The Data Protection Officer (DPO) has overall responsibility for this Policy and for ensuring all staff comply with it.

3 Our duties

3.1 We process personal information relating to individuals, including housing applicants, tenants (and their household members), factored owners, job applicants, current and former employees, contractors, business contacts, apprentices, committee members and members. As the controller of personal information, we have a responsibility under data protection legislation to protect the security of the personal information that we hold about data subjects.

3.2 We must keep personal information secure against loss or misuse. All staff are required to comply with this Policy and our Data Protection Policy and Information Security Policy.

4 What can cause a personal data breach?

A personal data breach can happen for several reasons:

4.1 loss or theft of equipment on which personal information is stored e.g. loss of a laptop or a paper file;

4.2 inappropriate access controls allowing unauthorised use of personal information;

4.3 equipment failure on which personal information is stored;

4.4 human error e.g. sending an e-mail containing personal information to the incorrect recipient;

4.5 unforeseen circumstances, such as damage to personal information due to a fire or flood;

4.6 hacking, phishing and other “blagging” attacks where personal information is obtained by deceiving whoever holds it;

4.7 alteration of personal information without permission; and

4.8 loss of availability of personal information.

5 If a personal data breach is discovered

5.1 If a member of staff knows or suspects that a personal data breach has occurred or may occur, they should contact the DPO immediately.

5.2 Staff should not take any further action in relation to the breach. Staff must not notify any affected data subjects or regulators. The DPO will take appropriate steps to deal with the breach in collaboration with the Data Breach Team.

6 Managing and recording the breach

6.1 On being notified of a suspected personal data breach, the DPO will notify the Data Breach Team, consisting of the DPO, Chief Executive and Director of Finance & Corporate Services. The Data Breach Team will be led by the DPO.

6.2 The Data Breach Team will take immediate steps to establish whether a personal data breach has in fact occurred. If so, the Data Breach Team will take appropriate action to:

6.2.1 contain the data breach and (so far as reasonably practicable) recover, rectify or delete the personal information that has been lost, damaged or disclosed;

6.2.2 assess and record the breach in the data breach register;

6.2.3 notify appropriate parties (including the Information Commissioner’s Office (ICO), Scottish Housing Regulator (SHR) and data subjects) of the breach; and

6.2.4 review the breach, its consequences and improvements that can be made.

These are explained in more detail below.

6.3 Containment and recovery

6.3.1 The Data Breach Team will within 24 hours of knowledge, where possible, identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal information.

6.3.2 The Data Breach Team will identify ways to recover, correct or delete personal information. This may include contacting the Police e.g. where the breach involves stolen hardware or personal information.

6.3.3 Depending on the nature of the breach, the Data Breach Team will notify our insurer, as the insurer can provide access to data breach management experts, who may be able to assist us.

6.4 Assess and record the breach

6.4.1 Having dealt with containment and recovery within 48 hours of knowledge, the Data Breach Team will assess the risks associated with the breach, including:

(a) what type of personal information is involved?

(b) is the personal information, sensitive personal information?

(c) who is affected by the breach i.e. the categories and approximate number of data subjects involved?

(d) the likely consequences of the breach on affected data subjects e.g. what harm could come to those data subjects, are there risks to their physical safety, reputation, or financial loss?

(e) where personal information has been lost or stolen, are there any protections in place, such as encryption?

(f) what has happened to the personal information e.g. if personal information has been stolen, could it be used for harmful purposes?

(g) what could the personal information tell a third party about the data subject e.g. could the loss of apparently trivial snippets of personal information help a determined fraudster build up a detailed picture of the data subject and result in e.g. identity theft?

(h) what are the likely consequences of the personal data breach on our organisation e.g. loss of reputation or liability for fines?

(i) are there wider consequences to consider e.g. loss of public confidence in an important service that we provide?

6.4.2 Details of the breach will be recorded in the data breach register by the Data Breach Team.

6.5 Notifying appropriate parties of the breach

6.5.1 The Data Breach Team will consider whether to notify:

(a) the ICO;

(b) affected data subjects;

(c) the Police; and

(d) other parties, including the SHR.

6.5.2 **Notifying the ICO**

(a) The Data Breach Team will notify the ICO when a personal data breach has occurred, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

(b) Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

(c) If the Data Breach Team is unsure whether to report, the presumption should be to report. The Data Breach Team will take account of the factors set out below:

The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a personal data breach should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include: —exposure to identity theft through the release of non-public identifiers e.g. passport number; and —information about the private aspects of the data subject's life becoming known to others e.g. financial circumstances.
The volume of personal information	There should be a presumption to report to the ICO where: —a large volume of personal information is concerned; and —there is a real risk of data subjects suffering some harm.

	It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high e.g. because of the circumstances of the loss or the extent of information about each data subject.
The sensitivity of personal information	There should be a presumption to report to the ICO where smaller amounts of personal information are involved, the release of which could cause a significant risk of data subjects suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves sensitive personal information. In these circumstances, even a single record could trigger a report.

6.5.3 **Notifying data subjects**

(a) Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Breach Team will notify the affected data subjects without undue delay, including:

(i) the name and contact details of the DPO from whom more information can be obtained;

(ii) the likely consequences of the personal data breach; and

(iii) the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

(b) When determining whether and how to notify data subjects of the personal data breach, the Data Breach Team will:

(i) co-operate closely with the ICO and other relevant authorities e.g. the Police; and

(ii) take account of the factors set out in the table below:

Factor	Impact on obligation to notify data subject
Whether we have implemented and applied (to the affected personal information) appropriate technical and organisational protection measures — in particular, measures that render the personal information unintelligible to any person who is not authorised to access it by e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject.
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject.
Whether it would involve disproportionate effort to notify the data subject.	If so, it is not necessary to notify the data subject — but we must instead issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject in any event.

6.5.4 **Notifying the Police**

The Data Breach Team will already have considered whether to contact the Police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the Data Breach Team will notify the Police and/or relevant law enforcement authorities.

6.5.5 **Notifying other parties**

The Data Breach Team will consider whether there are any legal or contractual requirements to notify any other parties, such as the SHR. We must report certain

notifiable events to the SHR, including a serious breach of legislation. Depending on the circumstances, and subject to the advice of the DPO, a personal data breach may be regarded as a serious breach of data protection legislation and may therefore constitute a notifiable event to the SHR. The prior advice of the DPO must be obtained by staff in such circumstances.

6.6 Reviewing the breach and improvements

Once the personal data breach has been handled in accordance with this Policy, the Data Beach Team will within one month of handling the personal data breach:

6.6.1 establish what security measures were in place when the breach occurred;

6.6.2 assess whether technical or organisational measures can be implemented to prevent the breach happening again;

6.6.3 consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or guidance;

6.6.4 consider whether it is necessary to conduct a new, or revisit an existing, data protection impact assessment of the personal information processing that was the subject of the breach; and

6.6.5 update the data breach register.

7 Staff awareness and training

7.1 Staff training and awareness raising is key to reducing the risks and occurrence of personal data breaches.

7.2 We provide regular data protection training to staff:

7.2.1 at induction;

7.2.2 when there is any change to the law, regulation or our policy;

7.2.3 when significant new threats are identified; and

7.2.4 in the event of a personal data breach occurring from which staff could learn.

8 Reporting breaches

Prevention is always better than cure. Data security concerns may arise at any time and we encourage staff to report any concerns to the DPO as soon as possible and at the earliest possible stage. This helps us capture risks as they emerge, protect us from personal data breaches, and keep our processes up-to-date and effective.

9 Consequences of failure to comply

9.1 Failure to comply with this Policy puts us at risk. Failure to notify the DPO of an actual or suspected personal data breach is a very serious issue.

9.2 Staff may be liable to disciplinary action if they fail to comply with the provisions of this Policy.

9.3 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.

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

Last updated: January 2023

6. RESPONSE PROCEDURES FOR DATA SUBJECT ACCESS REQUESTS

RESPONSE PROCEDURES FOR DATA SUBJECT REQUESTS

1 Introduction

1.1 Data subjects have certain rights in respect of their personal information. When we, West of Scotland HA, process data subjects' personal information, we must respect those rights. These procedures provide a framework for responding to requests from data subjects exercising those rights. We will ensure that requests by data subjects covered by these procedures to exercise their rights in relation to their personal information are handled in accordance with data protection legislation.

1.2 Our Data Protection Officer (DPO) is responsible for handling and responding to data subject requests. Staff must forward any requests received by them to the DPO immediately on receipt, and should not attempt to handle and respond to requests themselves.

1.3 These procedures only apply to data subjects whose personal information we process, including housing applicants, tenants (and their household members), factored owners, job applicants, current and former employees, contractors, business contacts, apprentices, committee members and members.

2 Definitions

For the purposes of this Policy:

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; and
processing	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying personal information, or using or doing anything with it.

3 Responding to requests to access personal information

3.1 Data subjects have the right to request access to their personal information processed by us. Such requests are called subject access requests (SARs). When a data subject makes a SAR, we will take the following steps:

3.1.1 log the date on which the SAR was received (to ensure that the relevant timeframe of one month for responding to the SAR is met);

3.1.2 confirm the identity of the data subject who is the subject of the personal information. For example, we may request additional information from the data subject to confirm their identity;

3.1.3 search databases, systems, applications and other places where the personal information which is the subject of the SAR may be held; and

3.1.4 confirm to the data subject whether personal information of the data subject making the SAR is being processed.

3.2 If personal information of the data subject is being processed, we will provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

3.2.1 the purposes of the processing of their personal information;

3.2.2 the categories of personal information concerned (for example, name, contact details, bank account information and complaints);

3.2.3 the recipients or categories of recipient to whom the personal information has been or will be disclosed, such as our contractors and other service providers;

3.2.4 where possible, how long the personal information will be stored, in line with our Data Retention Policy;

3.2.5 the existence of the right to request rectification or erasure of personal information or restriction of processing of personal information or to object to our processing of their personal information;

3.2.6 the right to lodge a complaint with the Information Commissioner's Office (ICO) about our processing of their personal information);

3.2.7 where the personal information has not been collected from the data subject, any available information as to its source;

3.2.8 the existence of automated decision-making (if any) and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

3.2.9 where personal information is transferred outside the European Economic Area, details of the appropriate safeguards to protect the personal information after transfer.

3.3 We will also, unless there is an exemption (see Paragraph 10 below), provide the data subject with a copy of the personal information processed by us in a commonly used electronic form (unless the data subject either did not make the SAR by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the SAR. If the SAR is complex, or there are several SARs, we may extend the period for responding by up to a further two months. If we extend the period for responding, we will inform the data subject within one month of receipt of the SAR and explain the reason(s) for the delay.

3.4 Before providing the personal information to the data subject making the SAR, we will review the personal information requested to see if it contains the personal information of other data subjects. If it does, we may redact the personal information of those other data subjects prior to providing the data subject with their personal information, unless those other data subjects have consented to the disclosure of their personal information or it would be reasonable to disclose the personal information of the other data subjects to the data subject.

3.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, considering the administrative costs of providing the personal information, or refuse to act on the SAR altogether.

3.6 If we will not be responding to the SAR, we will inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the ICO.

4 Responding to requests to rectify personal information

4.1 Data subjects have the right to have their inaccurate personal information rectified. Rectification can also include having incomplete personal information completed, for example, by a data subject providing a supplementary statement regarding the information. Where such a request is made, we will, unless there is an exemption (see Paragraph 10 below), rectify the personal information without undue delay.

4.2 We will also communicate the rectification of the personal information to each recipient to whom the personal information has been disclosed (for example, our service providers who process the personal information on our behalf), unless this is impossible or involves disproportionate effort. We will also inform the data subject about those recipients if the data subject requests this information.

5 Responding to requests for the erasure of personal information

5.1 Data subjects have the right, in certain circumstances, to request that we erase their personal information. Where such a request is made, we will, unless there is an exemption (see Paragraph 5.5 and Paragraph 10 below), erase the personal information without undue delay if:

5.1.1 the personal information is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

5.1.2 the data subject withdraws their consent to the processing of their personal information and consent was the basis on which the personal information was processed and there is no other legal basis for the processing;

5.1.3 the data subject objects to the processing of their personal information on the basis of our performance of a task carried out in the public or our legitimate interests, which override the data subject's interests or fundamental rights and freedoms, unless we can either show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the personal information for the establishment, exercise or defence of legal claims;

5.1.4 the personal information has been unlawfully processed; or

5.1.5 the personal information must be erased to comply with the law.

5.2 When a data subject makes a request for erasure in the circumstances set out above, we will, unless there is an exemption (see Paragraph 5.5 and Paragraph 10 below), take the following steps:

5.2.1 log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

5.2.2 confirm the identity of the data subject who is the subject of the personal information. We may request additional information from the data subject to do this;

5.2.3 search databases, systems, applications and other places where the personal information which is the subject of the request may be held and erase such information within one month of receipt of the request. If the request is complex, or there are several requests, we may extend the period for responding by up to a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;

5.2.4 where we have made the personal information public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal information that the data subject has requested the erasure by them of any links to, or copies or replications of, that personal information; and

5.2.5 communicate the erasure of the personal information to each recipient to whom the personal information has been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

5.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, considering the administrative costs of erasure, or refuse to act on the request.

5.4 If we will not be responding to the request, we will inform the data subject of the reasons for not acting and of the possibility of lodging a complaint with the ICO.

5.5 In addition to the exemptions in Paragraph 10 below, we can also refuse to erase the personal information if we need to keep the personal information:

5.5.1 for exercising the right of freedom of expression and information;

5.5.2 to comply with the law or to perform a task carried out in the public interest;

5.5.3 for reasons of public interest in public health;

5.5.4 for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of those purposes; or

5.5.5 for the establishment, exercise or defence of legal claims.

6 Responding to requests to restrict the processing of personal information

6.1 Data subjects have the right, unless there is an exemption (see Paragraph 10 below), to restrict the processing of their personal information if:

6.1.1 the data subject contests the accuracy of the personal information, for a period to allow us to check the accuracy of their personal information;

6.1.2 the processing is unlawful, and the data subject opposes the erasure of the personal information and requests the restriction of its use instead;

6.1.3 we no longer need the personal information for the purposes we collected it for and intend to dispose of it, but the data subject requires it for the establishment, exercise or defence of legal claims; and

6.1.4 the data subject has objected to the processing, pending checking whether we have legitimate grounds to override the data subject's objection.

6.2 Where processing has been restricted, we will only process the personal information (excluding storing it):

6.2.1 with the data subject's consent;

6.2.2 for the establishment, exercise or defence of legal claims;

6.2.3 for the protection of the rights of another person; or

6.2.4 for reasons of important public interest.

6.3 Prior to lifting the restriction, we will inform the data subject of the lifting of the restriction.

6.4 We will communicate the restriction of processing of the personal information to each recipient to whom the personal information has been disclosed, unless this is impossible or involves disproportionate effort. We will also inform the data subject about those recipients if the data subject requests it.

7 Responding to requests for the portability of personal information

7.1 Data subjects have the right, in certain circumstances, to receive their personal information that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another organisation. Where such a request is made, we will, unless there is an exemption (see Paragraph 10 below), provide the personal information without undue delay if:

7.1.1 the legal basis for the processing of the personal information is consent or performance of a contract; and

7.1.2 we process that personal information in electronic format.

7.2 When a data subject makes a request for portability in the circumstances set out above, we will take the following steps:

7.2.1 log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

7.2.2 confirm the identity of the data subject who is the subject of the personal information. We may request additional information from the data subject to confirm their identity; and

7.2.3 search databases, systems, applications and other places where the personal information which is the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal information directly to another organisation, where technically feasible) within one month of receipt of the request. If the request is complex, or there are several requests, we may extend the period for responding by up to a further two months. If we extend the period for responding, we will inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

7.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, considering the administrative costs of providing or transmitting the personal information, or refuse to act on the request.

7.4 If we will not be responding to the request, we will inform the data subject of the reasons for not acting and of the possibility of lodging a complaint with the ICO.

8 Responding to objections to the processing of personal information

8.1 Data subjects have the right to object to the processing of their personal information where such processing is based on our performance of a task carried out in the public interest or based on our legitimate interests, which override the data subject's interests or fundamental rights and freedoms, unless we either:

8.1.1 can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or

8.1.2 are processing the personal information for the establishment, exercise or defence of legal claims.

8.2 Data subjects also have the right to object to the processing of their personal information for scientific or historical research purposes or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

8.3 Where such an objection is made, we shall, unless there is an exemption (see Paragraph 10 below), no longer process a data subject's personal information.

9 Responding to requests not to be subject to automated decision-making

Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the electronic processing of their personal information, if such decision produces legal effects concerning them or similarly significantly affects them. We do not take decisions based solely on the electronic processing of personal information.

10 Exemptions

10.1 The framework of exemptions from each of the above rights is complex, and it is the responsibility of the DPO to assess whether an exemption is relevant in any given circumstances.

Exemptions may apply from the above rights in the following circumstances (this list only sets out a selection of the exemptions):

10.1.1 the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

10.1.2 other important objectives of general national public interest and important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

10.1.3 the protection of the data subject or the rights and freedoms of others where the disclose by us of personal information about the data subject would involve disclosing personal information relating to another data subject identifiable from the information;

10.1.4 the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control;

10.1.5 the personal information is required to be disclosed by law or in connection with legal proceedings;

10.1.6 self-incrimination, where compliance would reveal evidence of the commission of an offence;

10.1.7 the personal information consists of a confidential reference for the purposes of the training, education or employment of the data subject;

10.1.8 management forecasting or planning in relation to our business; or

10.1.9 any negotiations that we have entered into with the data subject where disclosure would be likely to prejudice those negotiations.

7. DATA RETENTION POLICY

DATA RETENTION POLICY

1 Introduction

1. Our corporate information, records and data are important to how we conduct business and manage employees.

1.1 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.2 This Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.3 Failure to comply with this Policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.4 This Policy covers all data that we hold or have control over. This includes physical data, such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data, such as e-mails and electronic documents. It applies to both personal data and non-personal data. In this Policy, we refer to this information and these records collectively as “data”.This Policy also covers data that is held by third parties on our behalf, for example, cloud storage providers or offsite data storage.

2. Guiding principles

2.1 Through our data retention practices, we aim to meet the following commitments:

2.2 We comply with legal and regulatory requirements to retain data.

2.3 We comply with our data protection obligations, in particular, to keep personal data no longer than is necessary for the purposes for which it is processed.

2.4 We handle, store and dispose of data responsibly and securely.

2.5 We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.

2.6 We allocate appropriate resources, roles and responsibilities to data retention.

2.7 We regularly remind employees of their data retention responsibilities.

2.8 We regularly monitor and audit compliance with this Policy and update this Policy when required.

3. Role and responsibilities

3.1 We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised good practices. All employees must comply with this Policy. Failure to do so may subject us to serious civil and / or criminal liability.

3.2 Our Data Protection Officer (DPO) is responsible for identifying the proper period of retention for our data and for providing guidance and training to employees in relation to this Policy. Employees are, however, responsible for handling the destruction of data whose retention period has expired.

4. Recommended retention periods

4.1 Certain data is more important to us and is therefore listed in the recommended retention periods set out in the Schedule to this Policy as being required to be retained permanently. This may be because we have a legal requirement to retain it permanently (so that we can produce it in the future), or because we may need it as evidence of our transactions, or because it is important to the running of our business.

4.2 Some data may be discarded or deleted once it has served its useful purpose or the period for bringing any claims against us has expired. The recommended retention periods set out in the Schedule to this Policy specify time periods for the retention of such data. Such data must not be retained beyond this period, unless a valid and strong business reason justifies its continued retention. If employees are unsure whether to retain certain data beyond the recommended retention period, they should consult the DPO.

4.3 If data is not listed in the recommended retention periods set out in the Schedule to this Policy, employees should consult the DPO for guidance.

5. Disposal and destruction of data

5.1 Hard copy data must be destroyed by shredding and electronic data must be deleted securely. No hard copy data should be destroyed by recycling.

5.2 Data must not be destroyed if the DPO confirms that its continued retention is relevant and necessary for the purposes of legal proceedings in which we are involved.

6. Consequences of failure to comply

6.1 We take compliance with this Policy very seriously. Failure to comply with the Policy may lead to disciplinary action for an employee under our procedures, and this action may result in dismissal for gross misconduct.

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

SCHEDULE

RECOMMENDED DATA RETENTION PERIODS

Type of data	Recommended retention period
Governance and Management	
• Certificate of registration as a registered social landlord from SHR • Confirmation of registration as a Scottish charity from OSCR • Confirmation of charitable status from HMRC • Certificate of registration as a registered society with the FCA • Certificate of registration as a care provider with the Care Inspectorate • Rules and Standing Orders	Permanent
• Applications for membership	5 years from date of end of membership
• Full membership register • Abbreviated membership register • Register of share certificates • Register of tenant organisations	Permanent
• Board member declarations of interest • Board member documents, including appointment letters and bank details	6 years from end of membership
• Board (and AGM and SGM) minutes and resolutions (including special resolutions)	Permanent
• Board (and AGM and SGM) papers (including notice of Board meetings, AGMs and SGMs)	6 years from date of issue

Type of data	Recommended retention period
• Register of Board members	Permanent
• Register of payments and benefits • Register of gifts and hospitality	10 years from date of register entry
• Annual return on the Scottish Social Housing Charter, including supporting information	5 years from date of submission
• Annual return to the FCA	Permanent
• Business plans and supporting documentation • Business continuity plans	5 years from date of completion
• Risk registers	Permanent
Housing Management and Financial Inclusion / Income Maximisation	
• Housing application form (including equalities and medical information) • Tenancy offer letters • Tenant visit records • Tenancy agreement* • Emergency contact information / next of kin • Correspondence to and from tenants • Tenants' contact details • Tenants' identity documentation • Pet permissions • Alterations permissions • Changes to tenancy, including assignations, changes to joint tenancy, mutual exchange requests, sublets and succession forms and letters • Powers of attorney / mandates of authority	6 years from date of end of tenancy Information relating to children (as dependents) may be subject to extended data retention periods, depending on insurer's requirements. This could be up to 100 years after the last contact with the child. * Could retain the front page containing the tenant's name and the signature page of the original hard copy tenancy agreement, provided that a copy of the blank version of the standard tenancy agreement is retained. Some courts may accept an electronic / scanned version of the tenancy agreement, but

Type of data	Recommended retention period
• Guardianship documentation • Tenancy reference requests (received and provided) • Housing Benefit related documentation, including applications, claims (including reinstatement claims), consent mandates and correspondence to and from local authority Housing Benefit department • Universal Credit related documentation • Referrals for money and benefits advice • Correspondence to and from DWP • Correspondence to and from local authority Social Work department • Correspondence to and from support agencies • Occupational therapists' reports • Anti-social behaviour incidents, including Police reports, complaints, witness statements and noise recordings • End of tenancy form • Eviction case files • Void process documentation • Communications with local authority regarding allocations • Diary notes on document management system • Court letters, documents and notices of proceedings, court reports, correspondence with solicitors and correspondence to and from Shelter	this depends on how advanced the document management system is in terms of creating and retaining audit trails of scanned documents i.e. whether it is possible to prove beyond doubt that the scanned version is authentic and has not been altered following its scan to the document management system.
• Abandonment files	6 years from the date of last action
• Unsuccessful housing applications	5 years after notification of outcome of application

Type of data	Recommended retention period
• Tenant satisfaction surveys and consultations	3 years from date of completion
• Advice regarding benefits, debts arrears reduction and income maximisation, including details of referrals to, and contact with, other agencies	6 months from the date of last action
• Records of contact with children	Depends on the requirements of the insurer
Maintenance and Works	
• Gas servicing schedule • Decanting records • Inspection / complaint file notes	5 years from date of end of tenancy
• Housing Association Grant documentation for stage 3 adaptations • Correspondence with tenant re: works and adaptations • Works orders	5 years from date of completion of works
• Snagging reports	5 years from date of report
• Stock condition surveys	5 years from date of survey
• Electrical and gas safety inspections	6 years from date of inspection
• Insurance claims	Depends on the requirements of the insurer (but minimum of 5 years from date of claim)

Housing Support	
• Care and support plans	Permanent
• Contact notes • Occupancy agreement • Health and communication needs	5 years from date of end of occupancy
• Care Inspectorate inspection reports	5 years from the end of the period of inspection
Factoring	
• Factoring agreement	5 years from date of termination of factoring agreement
• Communal work requests	5 years from the date of completion of works
Finance, Pensions and Insurance	
• Accounting records (including cheque counterfoils, bank statements and reconciliations and charitable donations made) • Auditing records • Balance sheets and supporting documents • VAT records and correspondence • Invoices • Credit and debit notes • Cash records, including petty cash	7 years from the end of the relevant financial year

• Creditor and debtor accounts • Orders and delivery notes	
• Signed versions of accounts • Grant funding (HAG, etc.)	Permanent
• Budgets and internal financial reports	2 years from the end of the relevant financial year
• Tax returns	10 years from the end of the relevant financial year
• Tenant financial information, including bank details	7 years from the date of payment
• Rent payments and rent statements • Arrears correspondence • Debt recovery, earnings and bank arrestments • Bankruptcy information	5 years from date of end of tenancy
• Rent refunds	7 years from the date of refund
• Employee salary records, records of overtime, bonuses and benefits in kind • Pay As You Earn (PAYE) records, including wage sheets, deductions, working sheets, calculations of the PAYE income of employees and relevant payments to them, the deduction of tax from, or accounting for tax in respect of, such payments	7 years from date of termination of employment
• Employee bank account details	Termination of employment (once final payments have been made)
• Copies of notices to employees (e.g. P45, P60) • HMRC correspondence in relation to tax codes, pay and tax details • Travel and subsistence payments (including expense claims and	7 years after the end of the relevant financial year

payments), season ticket advances and loans to employees • Employee income tax records • Records of income on which National Insurance contributions are payable • Records of employer's and employee's National Insurance contributions • Correspondence with HMRC	
• National minimum wage requirements records, including hours worked	3 years, beginning with the day upon which the pay reference period immediately following that to which they relate ends
• Statutory sick, maternity, paternity and shared parental pay records, calculations, certificates or other evidence	3 years after the end of the relevant financial year
• Pension actuarial valuation reports • Returns of pension fund contributions • Annual reconciliations of pension fund contributions	Permanent
• Documentation relating to retirement benefits	6 years after the date of employee retirement
• Pensioner records and investment policies	12 years after end of benefits payable under policy
• Current and former insurance policies and certificates	Permanent
• Annual insurance schedules	6 years from the end of period of insurance

Information Requests and Complaints	
• GDPR subject access request register • Third party disclosure register • Environmental information request register	6 years from date of register entry
• GDPR subject access request case files, personal data provided, including legal advice and internal communications regarding request • Environmental information request case file, including record of correspondence with applicant and information provided	3 years from date of response / last contact
• Complaints to the Information Commissioner (GDPR) and the Scottish Information Commissioner (environmental information) • Complaints (including stage 2 complaints, correspondence with the SPSO and complaints performance reports) • Data security incident and breach investigation documentation	6 years from date of last action / report production / end of investigation
• GDPR general compliance records	3 years
• Data security incident and breach register	Permanent

Health and Safety	
• Health and safety assessments • Health and safety policy statements • Records of consultations with safety representatives	Permanent
• Health and safety statutory notices	6 years after compliance
• Records of reportable injuries, diseases or dangerous occurrences, including reportable incidents, reportable diagnoses and injury arising out of accident at work (and associated investigations and the accident book)	5 years from date of the entry
• Records of reportable injuries, diseases or dangerous occurrences, including reportable incidents, reportable diagnoses and injury arising out of accidents involving children (and associated investigations and the accident book)	Depends on the requirements of the insurer (but minimum of 25 years)
• Record of employees exposed to asbestos dust, including health records of each employee • Medical records and details of biological tests under the Control of Lead at Work Regulations • Medical records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record
• Records of monitoring of exposures to hazardous substances (where exposure monitoring is required under COSHH)	Where the record includes the personal exposures of identifiable employees, 40 years from the date of the last entry made in the record Otherwise, 5 years from the date of the last entry made in the record

• Records of tests and examinations of control systems and protective equipment under COSHH	5 years from the date on which the record was made
Recruitment and Human Resources	
• Rejected job applicant records, including application letters or forms (including equal opportunities monitoring forms), CVs (including copies of qualifications), references and other pre-employment checks, interview notes, assessment and psychometric test results and correspondence concerning application	6 months from date of notification of rejection
• Application records of successful candidates, including application letters or forms (including equal opportunities monitoring forms), CVs (including copies of qualifications), references and other pre-employment checks, interview notes, assessment and psychometric test results and correspondence concerning employment	7 years from date of termination of employment
• Criminal records requirement assessments for a particular post, including criminal records information forms, Disclosure Scotland and PVG checks and certificates	12 months after the assessment was last used All other information, as soon as practicable after the check has been completed and the outcome recorded, unless the DPO assesses – in exceptional circumstances – that retention is relevant to the ongoing employment relationship, in which case, maximum retention period of 6 months after the check has been completed

• Copies of identification documents	2 years from date of termination of employment
• Identification documents of foreign nationals (including right to work)	2.5 years from date of termination of employment
• Employment contracts, including personnel and training records, written particulars of employment and changes to terms and conditions of employment • Employee performance and conduct records, probationary period reviews, review meeting and assessment interviews, appraisals and evaluations and promotions and demotions • Death benefit nomination and revocation forms • Resignation, termination and retirement records • Grievances • Collective workforce agreements • Records concerning temporary employees	7 years from date of termination of employment
• Disciplinary investigations, including warnings	6 months after conclusion of investigation (at least 25 years in the case of disciplinary warnings involving children or vulnerable adults)
• Records relating to and / or showing compliance with Working Time Regulations, including registration of work and rest periods and working time opt-out forms	3 years from the date on which the record was made
• Annual leave records • Sickness records • Records of return to work meetings following sickness, maternity, etc.	7 years after the end of the relevant financial year

• Trade union agreements	10 years after ceasing to be effective
• Occupational health records	40 years after completion of assessment
• Redundancy records	7 years from date of redundancy
Contracts and Procurement	
• Transfer Agreement	30 years after the date of stock transfer
• Contracts executed under seal	20 years after the end of the contract
• Contracts for the supply of goods or services, including professional services • Documentation relating to small one-off purchases of goods and services where there is no continuing maintenance or similar requirement • Licensing agreements • Rental and hire purchase agreements • Indemnities and guarantees	6 years after the end of the contract
• Loan agreements • Right to buy sale documents	Permanent
• Forms of tender	6 years after notification of award decision
• Document relating to unsuccessful tenderers	3 years after contract award
• Documents relating to successful tenderers	6 years after the end of the contract

Property Records	
• Leases and titles to property	20 years after the end of the lease / ownership ceases
• Development documentation	20 years after settlement of all issues
• Wayleaves, licences and servitudes	20 years after the rights that were granted or received cease to exist
• Planning and building control permissions • Title searches undertaken prior to purchase of property	20 years after ownership ceases
• Property maintenance records	During ownership of property or 5 years after the maintenance works were undertaken, depending on whether ownership ceases before or after the 5 year period
• Reports and professional opinions on property-related matters	6 years after the report or professional opinion was issued

Vehicles	
• Ownership and registration documentation • Maintenance records, including MOT tests and servicing • Mileage records	2 years after the date of disposal of vehicle
PR, Communications and Website	
• Newsletter distribution lists (post)	Until the recipient opts out of receiving the newsletter
• Social media posts	Depends on internal business requirements
• Website contact forms / requests / enquiries / complaints	Delete as soon as the form / request / enquiry / complaint has been transferred to the document management system, although the original may be retained for audit trail purposes
• Photographs (including consent forms, where available)	Until the subject of the photograph objects to their photograph being used
Office and Administration	
• Visitor book entries	6 months from date of visit

8. CCTV POLICY

WEST OF SCOTLAND HOUSING ASSOCIATION

CCTV SYSTEMS POLICY

1. **Introduction**

1.1 WSHA owns and operates CCTV systems at various locations within its offices and housing stock. WSHA recognises its legal obligations in operating such systems and the rights and freedoms of those individuals whose images may be captured by the systems. WSHA is committed to operating CCTV systems fairly and lawfully at all times in accordance with, in particular, data protection and human rights laws.

1.2 WSHA considers that CCTV systems have a legitimate role to play in staff and public safety and crime prevention and detection. However, WSHA recognises that this may raise concerns about the effect on individuals and their privacy, as images captured by CCTV systems are personal data which must be handled and used by WSHA in accordance with data protection and human rights laws.

1.3 This Policy outlines why and how WSHA uses CCTV systems, how WSHA will handle and use personal data recorded by its CCTV systems, how WSHA will respond to requests for disclosure of captured images and for how long WSHA will retain captured images.

1.4 Responsibility for keeping this Policy up-to-date and advising WSHA on the use and operation of CCTV systems has been delegated to the Data Protection Officer (DPO).

2 **Principles**

2.1 WSHA will comply with the following principles when installing and operating CCTV systems:

2.1.1 CCTV systems will only be installed and operated where there is a clear identified and documented need and legal basis for their use.

2.1.2 Privacy by design will be the principal consideration when procuring new CCTV systems or if changes are to be introduced to existing systems by way of operation or the underlying technology.

2.1.3 CCTV systems will only be installed and operated after a data protection

impact assessment (DPIA) has been completed.

2.1.4 CCTV systems will be located to ensure that only necessary areas are captured by the systems and to minimise the capture of areas not relevant to the purposes for which the system has been installed, such as private homes, areas of private or neighbouring property.

2.1.5 CCTV systems will not capture sound.

2.1.6 CCTV systems will only capture images of a suitable quality for the purposes for which the systems have been installed.

2.1.7 CCTV systems will attach date and time stamps to captured images.

2.1.8 Appropriate technical and organisational measures will be put in place to ensure the security of CCTV systems and captured images and to protect the systems from vandalism. Controls will be implemented to govern access to and use of such images by authorised personnel only.

2.1.9 Appropriate measures will be taken to provide clear signage and information to individuals whose images are captured by the CCTV systems.

2.1.10 Captured images will only be retained for as long as is necessary for the purposes for which the CCTV systems have been installed.

3 Reasons for use of CCTV systems

WSHA uses CCTV systems for its legitimate business purposes, including to prevent and detect (and act as a deterrent against) crime and anti-social behaviour, to protect buildings and assets from damage, disruption, vandalism and other crime and to apprehend and prosecute offenders.

4 How WSHA will operate CCTV systems

4.1 WSHA will operate its CCTV systems, capture images and use captured images in accordance with the requirements of data protection law.

4.2 WSHA will ensure that clear and prominent signs are displayed where CCTV systems are in operation to alert individuals that their images may be captured. The signs will contain details of WSHA as the organisation operating the systems, the purpose for which WSHA has installed and uses the systems and contact details for further information. Supplementary information on WSHA use of CCTV systems is also available at the WSHA office.

4.3 Staff responsible for operating the CCTV systems will exercise care when using the systems. This includes positioning CCTV system cameras so as to not overlook areas that are not intended to be captured and operating the systems sensibly, professionally and lawfully, with respect for the general public and in accordance with this Policy and applicable laws. Staff will be provided with appropriate training on the

applicable laws, including on how to handle captured images securely and assist the DPO in responding to requests for captured images.

4.4 WSHA will retain detailed records in situations where captured images are removed from the place that they are normally stored (for example, when complying with paragraphs 6.6 and 6.7 of this Policy, for CCTV equipment maintenance or repair or for use during legal proceedings) of:

4.4.1 date and time of removal;

4.4.2 name of the person removing the images;

4.4.3 name of the person viewing the images, including any third parties;

4.4.4 reason for removing the images (if the images were removed for use in legal proceedings, the crime incident number should be noted);

4.4.5 outcome, if any, of the removal; and

4.4.6 date and time that the images were returned to the place from which they were removed or, if not returned, whether the images were retained for evidential purposes.

5 Requests for disclosure of captured images by third parties

5.1 No images captured by WSHA's CCTV systems will be disclosed to any third party, without the disclosure first being authorised by the DPO.

5.2 Images will not normally be released, unless there is demonstrable proof that they are required for crime prevention and detection, the apprehension and prosecution of offenders, legal proceedings or by court order. No captured images will be posted online or disclosed to the media.

5.3 WSHA will retain detailed records of the following when disclosing captured images to third parties (for example, the Police):

5.3.1 date and time at which access was allowed;

5.3.2 identification of any third party who was allowed access;

5.3.3 reasons for allowing access; and

5.3.4 details of the captured images to which access was allowed.

6 Individual requests for access to or erasure of captured images

6.1 Data protection law grants rights to individuals in relation to their personal data. This includes rights to request access to and erasure of their images captured by WSHA CCTV systems. Any request received must be forwarded to the DPO immediately for

handling and response.

6.2 To allow WSHA to handle and respond to requests and locate relevant captured images, requests must include:

6.2.1 date and time of the recording;

6.2.2 location where the images were captured; and

6.2.3 information to permit identification of the individual, if necessary.

6.3 In the case of access requests, individuals will be asked if they wish to view the captured images or would like a copy. Copies will be provided on USB memory stick, unless the individual expresses an alternative preference. Viewings of captured images will take place at the WSHA office where appropriate viewing facilities will be made available for this purpose.

6.4 WSHA retains copyright in all images captured by its CCTV systems. Any further use or publication of images provided to an individual in response to an access request is prohibited, unless the individual first obtains authorisation from WSHA.

6.5 WSHA is entitled to refuse access to captured images in limited circumstances, such as where disclosure would prejudice the prevention or detection of crime or the prosecution of offenders. Where captured images have been passed to the Police or Procurator Fiscal, an access request from an individual will be refused until such time as WSHA has been notified that no proceedings will be taken, or proceedings have concluded.

6.6 WSHA will edit, disguise or blur images of third parties when disclosing captured images in response to an access request to protect the interests of third parties captured in the images. If this is not possible, then WSHA will not disclose the captured images.

6.7 WSHA will only erase an individual's images from captured images in response to a request where there is no legal basis or purpose for WSHA to continue to hold the images. WSHA will ensure that the erasure of an individual's image will not affect the images of other individuals who have been captured by the CCTV system.

7 **DPIAs**

7.1 WSHA will complete DPIAs of existing CCTV systems at least once every 12 months to ensure that their use remains necessary and appropriate and they continue to address the needs that justified their initial installation and operation. Where the outcome of a DPIA is that the use of a CCTV system can no longer be justified as being necessary or proportionate, arrangements for the removal of the system, together with associated equipment and signage, will be made immediately.

7.2 Prior to introducing a new CCTV system, placing a CCTV system in a new location or implementing changes in how the CCTV system operates or the underlying

technology, WSHA will complete a DPIA to assess compatibility with the requirements of data protection law. The DPIA will assist WSHA in deciding if the new system, new location or changes in operation or technology are necessary and proportionate in the circumstances, whether they should be used or if limitations should be placed on their use in the light of risks. Consideration will be given to less privacy invasive alternatives, where available.

7.3 DPIAs will be completed in accordance with WSHA Data Protection Policy. The DPO will provide advice and assistance on DPIAs, as required.

8 Retention of captured images

8.1 Images captured by WSHA CCTV systems will be stored locally on hard disk drive and will be permanently and securely deleted after 30 days, unless continued retention is required for an ongoing issue, for example, the apprehension and prosecution of offenders or to respond to a request made by an individual under data protection law. In those situations, captured images will be retained for as long as is necessary for those purposes and steps will be taken to prevent their automatic deletion.

8.2 At the end of their useful life, hard disk drives and any physical matter, such as digital video files and hard copy prints, will be erased permanently and securely and destroyed by an external contractor, who will issue a certificate to confirm the same.

9 Complaints

Complaints about the use of WSHA CCTV systems should be forwarded to the DPO in the first instance. Complaints will be handled and responded to in accordance with the Complaints Policy.

10 Consequences of failure to comply

10.1 WSHA takes compliance with this Policy very seriously. Failure to comply with the Policy:

10.1.1 puts at risk the individuals whose images are captured by the CCTV systems;

10.1.2 carries the risk of sanctions for WSHA and associated significant reputational damage; and

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

10.2 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 WSHA procedures, and this action may result in dismissal for gross misconduct.

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

11 Review and updates to this Policy

WSHA will review and update this Policy and may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in law.

Last updated: January 2023

9. WEBSITE COOKIE POLICY

WEBSITE COOKIE POLICY

This policy contains important information on how we use cookies on our website.

Cookies

Cookies are small text files that are placed on your device by websites that you visit. They are widely used to make websites work or work more efficiently, as well as to provide information to the owners of the website. Some of this information will be aggregated or statistical, which means you will not be identified individually.

Cookies used on our website

Our website uses two types of cookies:

1. Required cookies: these enable core functionality of our website, such as security, network management and accessibility. We do not need your permission to place these cookies on your device.

2. Analytics cookies: these help us to improve our website by collecting and reporting information on how you use it. The cookies collect information in a way that does not directly identify anyone. We need your permission to place these cookies on your device. You can withdraw your permission at any time through the cookie control box at the bottom of every page on our website. You may need to refresh the page for the updated settings to take effect.

The table below provides more information about the cookies we use and why:

Cookie	Name	Purpose	Required Cookie?
Universal Analytics (Google)	*_ga, _gali, _gat, _gid*	Used to collect information about how visitors use our website. We use the information to compile reports and to help us improve the website. The cookies collect information in a way that does not	*No.*

Cookie	Name	Purpose	Required Cookie?
		directly identify anyone, including the number of visitors to the website, where visitors have come to the website from and the pages they visited. Read Google's overview of privacy and safeguarding data	

The above cookies will only be accessed by us and the named third parties for the above purposes and will not be accessed by any other third party.

How to refuse cookies

You may be able to change your Internet browser settings so that cookies (including required cookies) are not accepted. If you do this, you may lose some of the functionality of our website.

You can find out how to manage cookies on popular Internet browsers by clicking on the following links:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Microsoft Internet Explorer
- Opera
- Apple Safari

To find information relating to other browsers, please visit the Internet browser developer's website.

To opt out of being tracked by Google Analytics across all websites, visit http://tools.google.com/dlpage/gaoptout.

Contact us

We have appointed a Data Protection Officer (DPO), who ensures that we comply with data protection laws. If you have any questions about this statement or how we hold or use your personal information, please contact the DPO at: info@westscot.co.uk

You can also contact us by: telephone on 0141 550 5600 or writing to: West of Scotland Housing Association Limited, Camlachie House, Barrowfield Drive, Camlachie, Glasgow, G40 3QH.

If you would like to receive this policy in alternative format, for example, audio, large print or braille, please contact our DPO.

Updates to this policy

We may update this policy at any time, and you should check our website occasionally to ensure you are aware of the most recent version that will apply each time you access our website.

WEBSITE COOKIE CONTROL BOX

Our use of cookies

We use necessary cookies to make our site work. We would also like to set optional analytics cookies to help us improve it. We will not set optional cookies unless you enable them. Using this tool will set a cookie on your device to remember your preferences.

For more detailed information about the cookies we use, see our Cookie Policy

Necessary cookies

Necessary cookies enable core functionality, such as security, network management, and accessibility. You may disable these by changing your browser settings, but this may affect how the website functions.

Analytics cookies

We would like to set Google Analytics cookies to help us to improve our website by collecting and reporting information on how you use it. These cookies collect information in an anonymous form.

For more information on how these cookies work, please see our Cookie Policy

10. TEMPLATES & RESOURCES

HOW WE USE YOUR PERSONAL INFORMATION - STAFF

We, West of Scotland Housing Association, are the controller of the personal information that we hold about you, our employee. This means that we are legally responsible for how we hold and use personal information about you. It also means that we are required to comply with data protection laws when holding and using your personal information. This includes providing you with the details contained within this statement of how we hold and use your personal information, who we may share it with and your rights in relation to your personal information.

We have appointed a Data Protection Officer (DPO), who ensures that we comply with data protection laws. If you have any questions about this statement or how we hold or use your personal information, please contact the DPO at: info@westscot.co.uk.

You can also contact us by: telephone on 0141 550 5600; or writing to: West of Scotland Housing Association Limited, Camlachie House, Barrowfield Drive, Camlachie, Glasgow, G40 3QH.

Your attention is particularly drawn to section 3 of this statement, which confirms that you consent to your personal information and sensitive personal information being held and used by us as described in section 2 of this statement.

1. What personal information do we hold and use about you?

As part of your employment contract with us, we hold and use the personal information that you provide to us and / or other personal information that we may obtain about you from you and from third parties on an ongoing basis. This includes your:

- name;

- contact information, including emergency contact / next of kin information;
- date of birth;
- gender;
- financial information, including salary, benefits, pension arrangements, bank account details, National Insurance and tax information;
- marital status, date of name change and any dependents;
- photograph to identify you on our website, if applicable;
- nationality, passport number, immigration status and information from related documents, such as your passport or other immigration-related information;
- DVLA checks, driving licence, vehicle insurance and MOT status (if applicable) included within the annual driving return, if you need to drive a vehicle as part of your employment with us;
- recruitment information;
- biographical information (if applicable to your employment with us);
- recognition and awards;
- sickness and and other leave records;
- sensitive personal information about your racial or ethnic origin, sexual orientation, your physical and / or mental health (including details of any regular prescription drugs), religious or other similar beliefs and / or political opinions (where you choose to share this with us);
- criminal records information, including Disclosure Scotland and / or Protecting Vulnerable Groups scheme checks (if applicable to your employment with us);
- grievances and / or complaints raised by you or involving you and / or conduct or disciplinary issues involving you;
- appraisals and performance reviews;
- qualifications and training records;
- membership of professional bodies;time and attendance records;
- declarations of interest;
- signature (including electronic signature);
- references that we provide to others (on your request);
- your location information and conversations with third parties (if applicable), if you use the Guardian 24 service as apart of your employment with us; and
- clothing and footwear sizes (if the provision of clothing and footwear is applicable to your employment with us).

If you do not provide us with the above personal information, we may not be able to continue to employ you or to provide you with the benefits described in section 2 of this statement. We may also be prevented from complying with the laws that apply to us, for example, to ensure your health and safety.

2. Why do we hold and use this personal information about you?

We use such personal information to:

- meet our responsibilities under the employment contract between us;
- pay your salary and benefits and deduct tax, National Insurance and pension contributions;
- comply with taxation, reporting and regulatory requirements;
- make decisions about salary reviews, promotions and your continued employment;
- record absences, including the reason(s) for such absences;
- administer sick pay entitlement;
- determine your fitness to work;
- carry out right to work and other required statutory checks;
- process flexible leave, special leave, parental leave, adoption leave and homeworking requests;
- process requests for the partial reimbursement of the cost of spectacles;
- facilitate the completion by you of annual display screen equipment self-assessments;
- deal with disciplinary and grievance matters;
- monitor and manage staff performance, conduct and attendance;
- protect your vital interests, for example, to notify your next of kin and / or obtain emergency medical assistance in the case of an accident involving you;
- deliver education and training;
- ensure continuity of employment and service rights (if applicable);
- provide you with protective clothing and equipment;
- maintain our register of interests;
- check driving licence and vehicle status and insurance arrangements;
- comply with our legal duties and obligations as your employer and to comply with employment law requirements, our equal opportunity monitoring obligations, and health and safety laws, if you drive a vehicle as part of your employment with us;
- protect our personal information and systems and ensure business continuity;
- include information about you on our website and within other publications;
- undertake business management and planning, including accounting and auditing;
- check that you comply with restrictions on your activities that apply after your employment with us has terminated (if applicable);
- provide you with a reference; and
- protect and defend our legal rights in the case of a dispute between us.

3. What is our legal basis for holding and using your personal information?

Data protection laws require us to have a legal reason for holding and using your personal information. Our legal reasons for holding and using your personal information include:

- compliance with the employment contract between us;
- compliance with the laws which apply to us as an employer;
- protection of your vital interests; and
- protection of our legitimate interests – in the highly unlikely event that we do not have another legal reason, we may consider that we have a legitimate interest in handling and using your personal information, for example, to maintain employment records and protect and defend our legal rights. In those circumstances, we will always consider your legitimate interests in the protection of your personal information, and will balance those against our own legitimate interests in handling and using your personal information for the purposes described in section 2 of this statement.

In very limited circumstances, we may rely on your consent as the legal reason. By providing us with your personal information and sensitive personal information (including your racial or ethnic origin, sexual orientation, your physical and / or mental health, religious or other similar beliefs and / or political opinions) and the personal information and sensitive personal information of other individuals (for example, your emergency contact / next of kin or dependents), you:

- consent to it being used by us as described in section 2 of this statement; and
- confirm that you have informed the other individuals if they are of 12 years old and above of the content of this statement and they have provided their consent to their personal information and sensitive personal information being used by us as described in section 2 of this statement.

You and the individuals have the right to withdraw your consent to us holding and using your and their personal information and sensitive personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information and sensitive personal information for the purpose(s) set out in section 2 of this statement, which you originally agreed to, unless we have another legal reason for doing so.

4. Who do we share your personal information with?

We may share your personal information with the following organisations for the purposes described in section 2 of this statement:

- HM Revenue and Customs;
- Home Office;
- Health and Safety Executive;
- Disclosure Scotland;
- Scottish Housing Regulator in statistical format (or in identifiable format for senior positions);
- our financial advisers, consultants and IT service and platform providers;
- our solicitors;
- our auditors;
- our pension provider, the Scottish Housing Association Pension Scheme, if you do not opt out of auto enrolment;
- our insurers;
- your doctor and other medical professionals;
- occupational health professionals;
- any organisation to which you are seconded as part of your employment with us;
- your previous employer for continuity of employment and service rights purposes (if your previous employer was an RSL and an EVH member);
- the Police (in the case of actual or suspected criminal activity);
- training providers, institutions and events providers;
- our clothing and footwear suppliers; and
- any other organisation that you authorise us to disclose your personal information to.

5. Where is your personal information transferred to?

Some of the organisations we share your personal information with (listed in section 4 of this statement) may be based or may make use of data storage facilities that are located outside the United Kingdom. Their handling and use of your personal information will involve us and / or them transferring it outside the United Kingdom. When we and / or they do this, we will ensure similar protection is afforded to it by:

- only transferring it or permitting its transfer to countries that have been deemed to provide an adequate level of protection for personal information under data protection laws; or
- using specific contracts with such organisations, which are approved for use in the United Kingdom, and which give your personal information the same protection it has in the United Kingdom after it is transferred.

Please contact our DPO for further information on the specific mechanism used by us when transferring your personal information outside the United Kingdom.

6. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 2 of this statement, including to meet any legal, accounting, reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting our DPO.

7. What rights do you have in relation to your personal information that we hold and use?

It is important that the personal information that we hold about you is accurate and current. Please keep us informed of any changes. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.
- Correction of any incomplete or inaccurate personal information that we hold about you.Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it or to stop us from using your personal information altogether if we have committed a breach of data protection laws.
- The transfer of your personal information to another organisation, for example, the transfer of your training record to a future employer.

You can also object to us holding and using your personal information where our legal reason is a legitimate interest (either our legitimate interests or those of a third party).

Please contact our DPO if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

8. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to our DPO.

You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The ICO's contact details are as follows:

Telephone: 0303 123 1113 Website: https://ico.org.uk/concerns/

If you would like to receive this statement in alternative format, for example, audio, large print or braille, please contact us.

9. Updates to this statement

We may update this statement at any time, and we will provide you with an updated version when required to do so by law.

WEST OF SCOTLAND HOUSING ASSOCIATION LIMITED

HOW WE USE YOUR PERSONAL INFORMATION - TENANTS

We, West of Scotland HA, are the controller of the personal information that we hold about you, which means that we are legally responsible for how we hold and use personal information about you. It also means that we are required to comply with data protection laws when holding and using your personal information.

We have appointed a Data Protection Officer (DPO), who ensures that we comply with data protection laws. If you have any questions about this statement or how we hold or use your personal information, please contact the DPO at: info@westscot.co.uk
You can also contact us by: telephone on 0141 550 5600; or writing to: West of Scotland Housing Association Limited, Camlachie House, Barrowfield Drive, Camlachie, Glasgow, G40 3QH.

Your attention is particularly drawn to section 2 of this statement, which confirms that you consent to your personal information and sensitive personal information being held and used by us as described in section 1 of this statement.

1. What personal information do we hold and use about you and why?

As part of your tenancy agreement with us, we hold and use the personal information that you provided to us in your housing application form, that the third parties who referred you to us provided to us and / or other personal information that we may obtain about you from you and third parties on an ongoing basis.

We use such personal information for the following purposes:

- providing you with services as the landlord of your property;
- communicating with you, including in response to any of your enquiries;
- improving our services and responding to changing needs;
- tenancy management and administration, including: processing your rent payments (including entering into rent payment arrangements with you); carrying out repairs to your property (including recharging such repairs to you, if relevant); assessing your housing needs; making special adaptations to your property; completing safety and other periodic maintenance checks to your property; handling and resolving complaints made by / against you; and recovering any rent arrears;
- keeping the personal information that we hold about you accurate and up-to-date;
- completing satisfaction surveys and surveys to obtain more detailed information about your household;

- complying with our legal and statutory duties, including those contained within the Equality Act 2010;
- publishing our newsletter and other communications in hard copy format, on social media and on our website;
- allowing you to take part in our tenant participation and engagement activities (if you choose to do so);
- preparing and submitting our annual return on the Scottish Social Housing Charter to the Scottish Housing Regulator;
- providing you with benefits, budgeting and debt advice and signposting you to organisations that can offer further advice and support;
- determining whether you are to be classed as a "no lone visit", based on our assessment of your conduct and / or the complaints that we have received about you;
- assisting with crime prevention and detection;
- protecting individuals from harm;
- compiling statistical information and returns to our Board and the Scottish Housing Regulator; and
- providing a reference on request if you move to another landlord.

2. What is our legal basis for holding and usinyour personal information?

By providing us with your personal information and sensitive personal information (relating to your health, racial or ethnic origin, religious or other beliefs or sexual orientation) and the personal information and sensitive personal information of other members of your household, you:

- consent to it being used by us as described in section 1 of this statement; and
- confirm that you have informed the other members of your household over the age of 12 years old of the content of this statement and they have provided their consent to their personal information and sensitive personal information being used by us as described in section 1 of this statement.

You and the other members of your household have the right to withdraw your consent to us holding and using your and their personal information and sensitive personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information and sensitive personal information for the purpose(s) set out in section 1 of this statement, which you originally agreed to, unless we have another legal basis for doing so.

Our other legal bases for holding and using your personal information are:

- performance and management of the tenancy agreement between us;
- legal and regulatory obligations which apply to us as a registered social landlord;
- protection of your vital interests; and
- our legitimate interests – while you have a legitimate interest in the protection of your personal information, we also have an overriding legitimate interest in handling and using your personal information, including sharing it with our contractors and service providers (listed in section 3 of this statement), for the purposes described in section 1 of this statement.

3. Who do we share your personal information with?

We share your personal information with the following organisations for the purposes described in section 1 of this statement:

- Repairs 24 and other contractors to undertake repairs, works and maintenance;
- the Willowacre Trust and the Department for Work and Pensions for benefits advice and support;
- our service providers to maintain the systems on which your personal information is stored, including our housing management software, and to allow you to make rent payments to us;
- utility companies to manage the payment of utilities for your property;
- compliance with our obligations under the data sharing agreements that we have entered into with local authorities;
- Bield Housing (if you are a tenant of sheltered housing) for emergency support;
- Community Safety Glasgow and other similar bodies in the local authority areas in which we operate for complaint resolution purposes;
- our Solicitors for providing advice on debt recovery actions, anti-social behaviour and evictions;
- our debt collection and tracing agents for the recovery of rent arrears;
- Police Scotland, Scottish Fire and Rescue Service and local authorities' anti-social behaviour departments, if you engage in anti-social or other criminal behaviour while our tenant;
- Scottish Public Services Ombudsman as part of our complaints procedure;
- third parties who undertake mailings on our behalf; and
- Research Resource to undertake tenant satisfaction surveys on our behalf.

4. Where is your personal information transferred to?

Some of the organisations we share your personal information with (listed in section 3 of this statement) may be based or may make use of data storage facilities that are located outside the United Kingdom. Their handling and use of your personal information will involve us and / or them transferring it outside the United Kingdom. When we and / or they do this, we will ensure similar protection is afforded to it by:

- only transferring it or permitting its transfer to countries that have been deemed to provide an adequate level of protection for personal information under data protection laws; or
- using specific contracts with such organisations, which are approved for use in the United Kingdom, and which give your personal information the same protection it has in the United Kingdom after it is transferred.

Please contact our DPO for further information on the specific mechanism used by us when transferring your personal information outside the United Kingdom.

5. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 1 of this statement, including to meet any legal, accounting,

reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting our Data Protection Officer (DPO).

6. What rights do you have in relation to your personal information that we hold and use?

It is important that the personal information that we hold about you is accurate and current. Please keep us informed of any changes by contacting our DPO. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.
- Correction of any incomplete or inaccurate personal information that we hold about you.
- Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it.
- The transfer of your personal information to another organisation.

You can also object to us holding and using your personal information where our legal basis is a legitimate interest (either our legitimate interests or those of a third party).

Please contact our DPO if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

7. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to our DPO.

You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The Information Commissioner's website is https://ico.org.uk/ and complaints can be made here.

8. Updates to this statement

We may update this statement at any time, and we will provide you with an updated version when are required to do so by law.

Last updated: January 2023

WEST OF SCOTLAND ASSOCIATION LIMITED

HOW WE USE YOUR PERSONAL INFORMATION – FACTORED OWNERS

We, West of Scotland HA, are the controller of the personal information that we hold about you, which means that we are legally responsible for how we hold and use personal information about you. It also means that we are required to comply with data protection laws when holding and using your personal information.

We have appointed a Data Protection Officer (DPO), who ensures that we comply with data protection laws. If you have any questions about this statement or how we hold or use your personal information, please contact the DPO at: info@westscot.co.uk.

You can also contact us by: telephone on 0141 550 5600; or writing to: West of Scotland Housing Association Limited, Camlachie House, Barrowfield Drive, Camlachie, Glasgow, G40 3QH.

Your attention is particularly drawn to section 2 of this statement, which confirms that you consent to your personal information and sensitive personal information being held and used by us as described in section 1 of this statement.

9. What personal information do we hold and use about you and why?

As part of your factoring agreement with us, we hold and use the personal information that you provided to us and / or other personal information that we may obtain from you when you contact us and / or complete an "Owner / Occupier Update" form and from third parties on an ongoing basis.

We use such personal information for the following purposes:

- complying with our legal duties and responsibilities as a registered property factor;
- providing you with services as the factor of your property;
- communicating with you, including to: respond to your enquiries, requests for information, policies and documents and complaints; notify you of any major repairs required to the common parts of the building in which your property is located; invite you to attend owners' meetings; and ask you to complete satisfaction surveys;
- providing you with a copy of the written statement of services, including any updates to the statement;improving our services and responding to changing needs;
- factoring management and administration, including record keeping, carrying out repairs to the common parts of the building in which your property is located

(including informing you about progress of the same) and processing your common charges and / or service charge invoices and payments;
- recovering any outstanding charges from you;
- keeping the personal information that we hold about you accurate and up-to-date;
- protecting and defending our legal rights if you apply to the First Tier Tribunal (FTT) for Scotland (Housing and Property Chamber); and
- taking any action following the issue of a property factor enforcement order against us by the FTT.

10. What is our legal basis for holding and using your personal information?

Data protection laws require us to have a legal reason for holding and using your personal information.

In some circumstances, we may rely on your consent as the legal reason. By providing us with your personal information and sensitive personal information (relating to your health, racial or ethnic origin, religious or other beliefs or sexual orientation) and the personal information and sensitive personal information of other members of your household (for example, an alternative contact in the event of an emergency), you:

- consent to it being used by us as described in section 1 of this statement; and
- confirm that you have informed the other members of your household of 12 years old and above of the content of this statement and they have provided their consent to their personal information and sensitive personal information being used by us as described in section 1 of this statement.

You and the other members of your household have the right to withdraw your consent to us holding and using your and their personal information and sensitive personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information and sensitive personal information for the purpose(s) set out in section 1 of this statement, which you originally agreed to, unless we have another legal reason for doing so.

Our other legal reasons for holding and using your personal information are:

- performance and management of the factoring agreement between us;
- legal and regulatory obligations which apply to us as a property factor;
- protection of your vital interests; and
- our legitimate interests – while you have a legitimate interest in the protection of your personal information, we also have an overriding legitimate interest in handling and using your personal information, including sharing it with our contractors and service providers (listed in section 3 of this statement), for the purposes described in section 1 of this statement.

11. Who do we share your personal information with?

We share your personal information with the following organisations for the purposes described in section 1 of this statement:

- our contractors to undertake repairs, works and maintenance to the common parts of the building in which your property is located;
- our service providers to maintain the systems on which your personal information is stored and to allow you to make payments of charges to us;
- our Solicitors for providing advice on debt recovery actions;
- your Solicitor to recover any outstanding charges when you sell your property;our debt collection and tracing agents for the recovery of charges payments;
- Research Resource to undertake owner satisfaction surveys on our behalf; and
- the FTT, if you apply to the FTT.

If the management of your property is to be transferred to a new property factor, then we will provide your personal information to the new property factor. This personal information will include your contact details and information about any ongoing and outstanding complaints.

12. Will my personal information be sent outside the UK?

Some of the organisations who we share your personal information with (listed in section 3 of this statement) may be based or may make use of data storage facilities that are located outside the UK. Their handling and use of your personal information will involve us and / or them transferring it outside the UK. When we and / or they do this, we will ensure similar protection is afforded to it by:

- only transferring it or permitting its transfer to countries that have been deemed to provide an adequate level of protection for personal information as a matter of data protection law; or
- using specific contracts with such organisations, which are approved for use in the UK, and which give your personal information the same protection it has in the UK.

Please contact our DPO for further information on the specific mechanism used by us when transferring your personal information outside the UK.

13. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 1 of this statement, including to meet any legal, accounting, reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting our DPO.

14. What rights do you have in relation to your personal information that we hold and use?

It is important that the personal information that we hold about you is accurate and current. Please keep us informed of any changes by contacting our DPO. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.

- Correction of any incomplete or inaccurate personal information that we hold about you.
- Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it.
- The transfer of your personal information to another organisation.

You can also object to us holding and using your personal information where our legal basis is a legitimate interest (either our legitimate interests or those of a third party).

Please contact our DPO if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

15. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to our DPO.

You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The ICO's contact details are as follows:

Telephone: 0303 123 1113 or Website: https://ico.org.uk/concerns/

If you would like to receive this statement in alternative format, for example, audio, large print or braille, please contact us.

16. Updates to this statement

We may update this statement at any time, and we will provide you with an updated version when are required to do so by law.

Last updated: January 2023

WEST OF SCOTLAND HOUSING ASSOCIATION LIMITED

HOW WE USE YOUR PERSONAL INFORMATION (HOUSING APPLICANTS)

We, West of Scotland HA, are the controller of the personal information that we hold about you. This means that we are legally responsible for how we hold and use personal information about you. It also means that we are required to comply with data protection laws when holding and using your personal information. This includes providing you with the details contained within this statement of how we hold and use your personal information, who we may share it with and your rights in relation to your personal information.

We have appointed a Data Protection Officer (DPO), who ensures that we comply with data protection laws. If you have any questions about this statement or how we hold or use your personal information, please contact the DPO at: info@westscot.co.uk

You can also contact us by: telephone on 0141 550 5600 or writing to: West of Scotland Housing Association Limited, Camlachie House, Barrowfield Drive, Camlachie, Glasgow, G40 3QH.

Your attention is particularly drawn to section 2 of this statement, which confirms that you consent to your personal information and sensitive personal information being held and used by us as described in section 1 of this statement.

17. What personal information do we hold and use about you and why?

We may need to hold and use the personal information that you provide to us as part of your housing application (including sensitive personal information about your health) and / or other personal information that we may obtain about you from you (for example, during a meeting with you) and from third parties (including your previous landlords and the local authority Social Work department, if applicable).

We hold and use this personal information to:

- process and manage your housing application;
- verify the information provided by you as part of your housing application, including your immigration and residency status;
- comply with legal requirements that apply to us as a registered social landlord in Scotland;
- comply with our equal opportunity monitoring obligations;
- compile anonymous statistical information on housing needs;
- communicate with and inform you of the outcome of your housing application;

- allocate housing in accordance with our allocations policy and based on your needs and preferences;
- determine if you are to be referred to our Welfare Rights team or the Willowacre Trust;
- obtain references about you from your previous landlords (if applicable);
- provide you with appropriate advice about access to benefits, if you are offered a tenancy (proof of pre-settled or settled status will be required from EU citizens for this purpose);
- prevent and detect fraud and take steps to terminate your tenancy (if you are successful in your application and allocated a property), if fraud is later discovered; and
- otherwise protect and defend our legal rights in the case of a dispute between us.

18. What is our legal basis for holding and using your personal information?

Data protection laws require us to have a legal reason for holding and using your personal information. Our legal reasons for holding and using your personal information include:

- complying with the laws that apply to us as a registered social landlord in Scotland;
- taking steps to enter into a tenancy agreement with you, if your housing application is successful; and
- protecting our legitimate interests – in the highly unlikely event that we do not have another legal reason, we may have a legitimate interest in handling and using your personal information. In those circumstances, we will always consider your legitimate interests in the protection of your personal information, and will balance those against our own legitimate interests in handling and using your personal information for the purposes described in section 1 of this statement.

In very limited circumstances, we may rely on your consent as the legal reason. By providing us with your personal information and sensitive personal information (including your racial or ethnic origin, sexual orientation, your physical and / or mental health, religious or other similar beliefs and / or political opinions) and the personal information and sensitive personal information of other individuals (including other members of your household), you:

- consent to it being used by us as described in section 1 of this statement; and
- confirm that you have informed the other individuals if they are of 12 years old and above of the content of this statement and they have provided their consent to their personal information and sensitive personal information being used by us as described in section 1 of this statement.

You and the individuals have the right to withdraw your consent to us holding and using your and their personal information and sensitive personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information and sensitive personal information for the purpose(s) set out in section 1 of this statement, which you originally agreed to, unless we have another legal reason for doing so.

19. Who do we share your personal information with?

We may share your personal information with the following organisations for the purposes described in section 1 of this statement:

- law enforcement and fraud prevention agencies;
- third parties from whom we may seek more information about you and to verify the information provided by you as part of your housing application, including your doctor, previous landlords, the Home Office, relevant local authority and any organisations that have referred you to us;
- Scottish Housing Regulator;
- our consultants, advisers and IT service providers; and
- our solicitors.

20. Where is your personal information transferred to?

Some of the organisations we share your personal information with (listed in section 3 of this statement) may be based or may make use of data storage facilities that are located outside the United Kingdom. Their handling and use of your personal information will involve us and / or them transferring it outside the United Kingdom. When we and / or they do this, we will ensure similar protection is afforded to it by:

- only transferring it or permitting its transfer to countries that have been deemed to provide an adequate level of protection for personal information under data protection laws; or
- using specific contracts with such organisations, which are approved for use in the United Kingdom, and which give your personal information the same protection it has in the United Kingdom after it is transferred.

Please contact our DPO for further information on the specific mechanism used by us when transferring your personal information outside the United Kingdom.

21. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 1 of this statement, including to meet any legal, accounting, reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting our DPO.

22. What rights do you have in relation to your personal information that we hold and use?

It is important that the personal information that we hold about you is accurate and current. Please keep us informed of any changes. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.
- Correction of any incomplete or inaccurate personal information that we hold about you.

- Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it or to stop us from using your personal information altogether if we have committed a breach of data protection laws.
- The transfer of your personal information to another organisation.

You can also object to us holding and using your personal information where our legal reason is a legitimate interest (either our legitimate interests or those of a third party).

Please contact our DPO if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

23. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to our DPO.

You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The ICO's contact details are as follows:

Telephone: 0303 123 1113

Website: https://ico.org.uk/concerns/

If you would like to receive this statement in alternative format, for example, audio, large print or braille, please contact us.

24. Updates to this statement

We may update this statement at any time, and we will provide you with an updated version when required to do so by law.

Last updated: January 2023

WEST OF SCOTLAND HOUSING ASSOCIATION LIMITED

HOW WE USE YOUR PERSONAL INFORMATION – BOARD MEMBERS

We, West of Scotland HA, are the controller of the personal information that we hold about you in your capacity as a Board member. This means that we are legally responsible for how we hold and use personal information about you. It also means that we are required to comply with data protection laws when holding and using your personal information. This includes providing you with the details contained within this statement of how we hold and use your personal information, who we may share it with and your rights in relation to your personal information.

We have appointed a Data Protection Officer (DPO), who ensures that we comply with data protection laws. If you have any questions about this statement or how we hold or use your personal information, please contact the DPO at: info@westscot.co.uk
You can also contact us by: telephone on 0141 550 5600; or writing to: West of Scotland Housing Association Limited, Camlachie House, Barrowfield Drive, Camlachie, Glasgow, G40 3QH.

Your attention is particularly drawn to section 3 of this statement, which confirms that you consent to your personal information being held and used by us as described in section 2 of this statement.

25. What personal information do we hold and use about you?

As part of your membership of the Board, we hold and use the personal information that you provide to us and / or other personal information that we may obtain about you from you and from third parties on an ongoing basis. This includes your:

- name;
- contact information;
- bank details;
- date of birth;
- nationality;
- occupation and employer;
- recruitment information;
- declarations of your interests regarding related parties and organisations;
- absence records, including leave of absence requests and reasons;
- grievances and / or complaints raised by you or involving you and / or conduct or disciplinary issues involving you;
- relevant skills and experience;

- membership of professional bodies and local groups;
- education and qualifications;
- appraisals, performance reviews and planning; and
- training records, including courses attended, strategies and plans.

If you are a tenant, then we will also hold and use your personal information in accordance with the "How We Use Your Personal Information" statement issued to our tenants.

If you do not provide us with the above personal information, you may not continue to be a Board member. We may also be prevented from complying with the laws that apply to us, for example, to ensure your health and safety.

26. Why do we hold and use this personal information about you?

We use such personal information to:

- manage and administer your membership of the Board;
- comply with regulatory requirements and our legal duties and obligations;
- pay your expenses for attendance at Board meetings;
- promote equality of opportunity;
- record absences, including the reason(s) for such absences;
- carry out required statutory checks;
- deal with disciplinary and grievance matters;
- monitor and manage your performance, conduct, development and attendance;
- protect your vital interests, for example, to notify your next of kin and / or obtain emergency medical assistance in the case of an accident involving you;
- deliver education and training;
- protect our personal information and systems and ensure business continuity;
- undertake business management and planning, including accounting and auditing; and
- protect and defend our legal rights in the case of a dispute between us.

27. What is our legal basis for holding and using your personal information?

Data protection laws require us to have a legal reason for holding and using your personal information. Our legal reasons for holding and using your personal information include:

- compliance with the laws which apply to us as a registered social landlord in Scotland;
- protection of your vital interests; and
- protection of our legitimate interests – in the highly unlikely event that we do not have another legal reason, we may consider that we have a legitimate interest in handling and using your personal information, for example, to maintain our records. In those circumstances, we will always consider your legitimate interests in the protection of your personal information, and will balance those against our own legitimate interests in handling and using your personal information for the purposes described in section 2 of this statement.

In very limited circumstances, we may rely on your consent as the legal reason. By providing us with your personal information and / or the personal information of other individuals, you:

- consent to it being used by us as described in section 2 of this statement; and
- confirm that you have informed the other individuals if they are of 12 years old and above of the content of this statement and they have provided their consent to their personal information being used by us as described in section 2 of this statement.

You and the individuals have the right to withdraw your consent to us holding and using your and their personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information for the purpose(s) set out in section 2 of this statement, which you originally agreed to, unless we have another legal reason for doing so.

28. Who do we share your personal information with?

We may share your personal information with the following organisations for the purposes described in section 2 of this statement:

- Scottish Housing Regulator;
- Office of the Scottish Charity Regulator;
- Financial Conduct Authority;
- Disclosure Scotland;
- our financial advisers, consultants, advisers and IT service providers;
- our solicitors;
- our auditors;
- our insurers; and
- the Police (in the case of actual or suspected criminal activity).

29. Where is your personal information transferred to?

Some of the organisations we share your personal information with (listed in section 4 of this statement) may be based or may make use of data storage facilities that are located outside the United Kingdom. Their handling and use of your personal information will involve us and / or them transferring it outside the United Kingdom. When we and / or they do this, we will ensure similar protection is afforded to it by:

- only transferring it or permitting its transfer to countries that have been deemed to provide an adequate level of protection for personal information under data protection laws; or
- using specific contracts with such organisations, which are approved for use in the United Kingdom, and which give your personal information the same protection it has in the United Kingdom after it is transferred.

Please contact our DPO for further information on the specific mechanism used by us when transferring your personal information outside the United Kingdom.

30. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 2 of this statement, including to meet any legal, accounting, reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting our DPO.

31. What rights do you have in relation to your personal information that we hold and use?

It is important that the personal information that we hold about you is accurate and current. Please keep us informed of any changes. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.
- Correction of any incomplete or inaccurate personal information that we hold about you.
- Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it or to stop us from using your personal information altogether if we have committed a breach of data protection laws.
- The transfer of your personal information to another organisation.

You can also object to us holding and using your personal information where our legal reason is a legitimate interest (either our legitimate interests or those of a third party).

Please contact our DPO if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

32. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to our DPO.

You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The ICO's contact details are as follows:

Telephone: 0303 123 1113

Website: https://ico.org.uk/concerns/

If you would like to receive this statement in alternative format, for example, audio, large print or braille, please contact us.

33. Updates to this statement

We may update this statement at any time, and we will provide you with an updated version when required to do so by law.

Last updated: January 2023

West of Scotland Housing Association Limited

CCTV: Supplementary Information

At West of Scotland HA, your safety and security is of paramount importance to us. For these reasons, CCTV is installed at our premises.

This document contains supplementary information to our CCTV signs, which are displayed at our premises. It contains important information about how we protect the CCTV images that we record and, more importantly, your rights in relation to such images.

Data security

We have put in place appropriate security measures to prevent your CCTV images from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your CCTV images to those employees, agents, contractors and other third parties who have a business or legal need to know. They will only handle your CCTV images on our instructions and subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any relevant regulator of a suspected breach where we are legally required to do so.

Data retention

We will only keep your CCTV images for as long as necessary to fulfil the purposes we collected them for and to comply with legal requirements.

Your rights relating to your CCTV images

Under certain circumstances, you have the right to:

- Request access to your CCTV images.
- Request the erasure of your CCTV images where there is no good reason for us continuing to use or hold them.

- Request the restriction of our use or holding of your CCTV images where you want us to determine our reason(s) for using or holding them as part of an erasure request (above).

- Request the transfer of your CCTV images to another party.

Please contact our Data Protection Officer (DPO) at info@westscot.co.uk 0141 550 5600 if you wish to make any of the above requests.

We may ask you for specific information to help us confirm your identity when making any of the above requests.

You will not be required to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

Right to withdraw consent

Where you have provided your consent to the recording of your images by CCTV, you have the right to withdraw your consent at any time. To withdraw your consent, please contact our DPO.

Once we have received notification that you have withdrawn your consent, we will no longer process your image by CCTV, unless we have another legal reason for doing so.

Feedback and complaints

We welcome your feedback on how we hold and use your CCTV images, and this can be sent to our DPO.

You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your CCTV images. The ICO's contact details are as follows:

Telephone: 0303 123 1113

Website: https://ico.org.uk/concerns/

If you would like to receive this statement in alternative format, for example, audio, large print or braille, please contact us.

Updates to this statement

We may update this statement at any time, and we will provide you with an updated version when required to do so by law.

Last updated: June 2018

CONTRACT ADDENDUM

ADDENDUM

1. In this Addendum, the following terms shall have the following meanings:

   a. "Contractor" means [INSERT NAME OF CONTRACTOR);

   b. "Controller", "Data Protection Impact Assessment", "Data Subject", "Information Commissioner's Office", "Personal Data", "Process" (including any derivatives thereof), "Processor", "and "Special Categories of Personal Data" shall each have the same meaning as defined in the Data Protection Laws; and

   c. "Data Protection Laws" means the General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018 and all applicable laws relating to processing of personal data and privacy.

2. In providing services to West of Scotland HA, the Contractor shall process such categories of personal data (including special categories of personal data) in relation to such categories of data subjects for and on behalf of West of Scotland HA as shall be strictly necessary for the provision of the services by the Contractor to West of Scotland HA and to perform and discharge the Contractor's obligations under this Addendum.

3. West of Scotland HA shall be the controller and the Contractor shall be the processor of all personal data that the Contractor processes in providing services to West of Scotland HA. The Contractor shall comply with the Data Protection Laws relating to the processing of personal data in providing services to West of Scotland HA.

4. The Contractor shall only process, and shall ensure that the Contractor's employees only process, the personal data in accordance with this Addendum and West of Scotland HA's written instructions from time to time, except where otherwise required by applicable law (and shall inform West of Scotland HA of that legal requirement in such case before processing, unless applicable law prevents it from doing so on important grounds of public interest).

5. The Contractor shall not transfer the personal data outside the United Kingdom without West of Scotland HA's prior written consent.

6. The Contractor shall at all times (at its own cost and expense) implement and maintain appropriate technical and organisational measures to protect the personal data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

7. The Contractor shall not permit the processing of the personal data by any subcontractor without the prior specific written authorisation of that subcontractor by West of Scotland HA and only then subject to such conditions as West of Scotland HA may require. Prior to the subcontractor processing the personal data, the Contractor must ensure that the subcontractor enters into a written agreement (to be approved by West of Scotland HA in advance) imposing on the subcontractor the same obligations as are imposed on the Contractor under this Addendum (and which are capable of being enforced directly by West of Scotland HA) and that the subcontractor complies with all such obligations. The Contractor shall remain fully liable to West of Scotland HA under this Addendum for all the acts and omissions of the subcontractor as if they were its own.

8. The Contractor shall ensure that all persons authorised by the Contractor or any subcontractor to process the personal data are:

    a. reliable and adequately trained in the Data Protection Laws;

    b. informed of the confidential nature of the personal data and that they must not disclose the personal data to any unauthorised party; and

    c. subject to a binding and enforceable written contractual obligation to keep the personal data confidential.

9. The Contractor shall (at its own cost and expense) promptly:

    a. provide such information and assistance (including by taking all appropriate technical and organisational measures) as West of Scotland HA may require in relation to the fulfilment of West of Scotland HA's obligations under the Data Protection Laws to respond to requests exercising data subjects' rights;

    b. provide such information, co-operation and other assistance to West of Scotland HA as West of Scotland HA requires to ensure compliance with West of Scotland HA's obligations under the Data Protection Laws, including in relation to: security of processing of the personal data; data protection impact assessments; prior consultation with the Information Commissioner's Office (or other supervisory authority) regarding high

risk processing; and any remedial action and / or notifications to be made or taken in response to any breach, complaint or request regarding either the Contractor's or West of Scotland HA's obligations under the Data Protection Laws relevant to this Addendum;

c. record and refer all requests and communications received from data subjects or the Information Commissioner's Office (or other supervisory authority) to West of Scotland HA which relate to the personal data and shall not respond to any such requests and communications without West of Scotland HA's express written approval and strictly in accordance with West of Scotland HA's instructions;

d. and (in any case) within 24 (Twenty Four) hours, notify West of Scotland HA if it or any subcontractor suspects or becomes aware of any suspected, actual or threatened occurrence of any breach of the Data Protection Laws in respect of any personal data and shall provide all information and assistance to West of Scotland HA as West of Scotland HA requires to report the breach to the Information Commissioner's Office (or other supervisory authority) and to notify affected data subjects under the Data Protection Laws; and

e. make available (and shall ensure that all subcontractors make available) to West of Scotland HA such information as is required to demonstrate the Contractor's and the subcontractor's compliance with their respective obligations under this Addendum and the Data Protection Laws, and allow for, permit and contribute to audits, including inspections by West of Scotland HA (or an auditor appointed by West of Scotland HA) for this purpose at West of Scotland HA's request from time to time.

10. The Contractor shall (and shall ensure that each of its subcontractors and employees shall) immediately, at West of Scotland HA's request, either securely delete or securely return all the personal data to West of Scotland HA in such form as West of Scotland HA requests after the earlier of:

a. the termination of the provision of services by the Contractor to West of Scotland HA; or

b. once processing of the personal data by the Contractor is no longer required for the performance of the Contractor's relevant obligations under this Addendum,

and securely delete existing copies of the personal data (except to the extent that the Contractor is required to retain the personal data by applicable law, in which case, the Contractor shall inform West of Scotland HA of any such requirement).

11. The Contractor shall indemnify and keep West of Scotland HA indemnified against all losses, claims, damages, liabilities, fines, interest, penalties, costs, charges, sanctions, expenses, compensation paid to data subjects, demands and legal and other professional costs (calculated on a full indemnity basis and, in each case, whether or not arising from any investigation by, or imposed by, the Information Commissioner's Office (or other supervisory authority) arising out of or in connection with any breach by the Contractor of its obligations under this Addendum and all amounts paid or payable by West of Scotland HA to a third party which would not have been paid or payable if the Contractor's breach of this Addendum had not occurred.

Subscribed for and on behalf of [INSERT NAME OF CONTRACTOR] by:

Name:

Signature:

At:

Date:

Witnessed by:

Name:

Signature:

Address:

Subscribed for and on behalf of West of Scotland HA by:

Name:

Signature:

At:

Date:

Witnessed by:

Name:

Signature:

Address:

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

WEBSITE PRIVACY POLICY

This website is operated by West of Scotland Housing Association. We, West of Scotland HA, take your privacy seriously and we ask that you read this policy carefully, as it contains important information on:

- the personal information we collect about you when you access our website;
- what we do with your personal information; and
- who your personal information might be shared with.

We are the controller of the personal information that we collect from you on our website, which means that we are legally responsible for how we collect, hold and use your personal information. It also means that we are required to comply with data protection laws when collecting, holding and using your personal information.

We have appointed a Data Protection Officer (DPO), who ensures that we comply with data protection laws. If you have any questions about this statement or how we hold or use your personal information, please contact the DPO at: info@westscot.co.uk

You can also contact us by: telephone on 0141 550 5600; or writing to: West of Scotland Housing Association Limited, Camlachie House, Barrowfield Drive, Camlachie, Glasgow, G40 3QH.

Your attention is particularly drawn to section 2 of this policy, which confirms that you consent to your personal information and sensitive personal information being held and used by us as described in section 1 of this policy.

34. What personal information do we collect about you and why?

Our website is a place for you to find out more about us, your neighbourhood and the services available to you.

When you visit our website, we collect personal information about you when you:

- enquire about or apply for housing with us;
- pay your rent;
- report a repair to us;
- apply to make alterations or improvements to your home, sublet, take in a lodger, assign your tenancy or keep a pet;
- request an adaptation to your home;

- notify us of any changes to your tenancy, including adding a joint tenant and changes to household members;
- inform us of changes to your contact details;
- complete a survey, including new tenant survey and satisfaction with repairs survey;
- provide us with notice to end your tenancy;
- apply for a garden waste permit;
- express an interest in getting involved as a tenant, owner or Committee member;
- make a complaint, report anti-social behaviour, notify us of estate management issues or otherwise provide your comments on the standard of service that you have received from us;
- submit an enquiry about any of the services listed on our website;
- complete and submit a "contact us" form to us; and
- submit an information request to us.

We use such personal information to:

- provide you with the information and services that you have requested from us;
- communicate with you, including in response to any of your enquiries or requests;
- improve our services and respond to changing needs;
- process your rent payments;
- carry out repairs to your property;
- handle and resolve complaints made by / against you;
- keep the personal information that we hold about you and members of your household accurate and up-to-date (if you provide any new personal information to us via the website); and
- arrange an appointment with our staff and / or any of the support services listed on our website.

We may not be able to provide the above services to you if you do not provide us with sufficient personal information to allow us to do so.

We may also collect information through the use of cookie files on our website. For further information on cookies, please see our Cookie Policy.

35. What is our legal basis for holding and using your personal information?

Data protection laws require us to have a legal reason for collecting, holding and using your personal information.

In some circumstances, we may rely on your consent as the legal reason. By providing us with your personal information and sensitive personal information (relating to your health, racial or ethnic origin, religious or other beliefs or sexual orientation) and the personal information and sensitive personal information of other members of your household via our website, you:

- consent to it being used by us as described in section 1 of this policy; and
- confirm that you have informed the other members of your household of 12 years old and above of the content of this policy and they have provided their consent to

their personal information and sensitive personal information being used by us as described in section 1 of this policy.

You and the other members of your household have the right to withdraw your consent to us holding and using your and their personal information and sensitive personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information and sensitive personal information for the purpose(s) set out in section 1 of this policy, which you originally agreed to, unless we have another legal reason for doing so.

Our other legal reasons for holding and using your personal information are:

- performance and management of the tenancy agreement between us;
- legal and regulatory obligations which apply to us as a registered social landlord;
- protection of your vital interests; and
- our legitimate interests – while you have a legitimate interest in the protection of your personal information, we also have an overriding legitimate interest in handling and using your personal information, including sharing it with our service providers (listed in section 3 of this policy), for the purposes described in section 1 of this policy.

36. Who do we share your personal information with?

We may share your personal information with the following organisations for the purposes described in section 1 of this policy:

- our contractors to undertake repairs, works and maintenance;
- our IT service providers, including the providers of our document management and housing management systems;
- organisations providing benefits advice and support; and
- local and other public authorities for housing management and regulatory purposes;
- Police Scotland and the local authority anti-social behaviour department in relation to complaints involving anti-social or other criminal behaviour.

37. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 1 of this policy, including to meet any legal, accounting, reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting our DPO.

38. How do we keep your personal information secure?

The security of your personal information is important to us and we use technical and organisational measures to safeguard your personal information.

However, while we will use reasonable efforts to safeguard your personal information, the use of the Internet is not entirely secure and, for this reason, we cannot guarantee the security of any personal information that is transferred by or to you via the Internet.

If you have any concerns about the security of your personal information, please contact our DPO for more information.

39. What if you provide us with personal information about somebody else?

We understand that there may be situations where you provide us with personal information about somebody else. In those situations, you confirm that:

- the other individual has consented to you acting for them and to your use of their personal information;

- you have informed the other individual of our identity and the contents of this policy, including the purposes for which we will use that individual's personal information described in section 1 of this policy; and

- the other individual has explicitly consented to our use of that individual's personal information for the purposes described in section 1 of this policy.

This policy will apply to our collection, handling and use of the other individual's personal information in the same manner that it applies to your own personal information.

40. Where is your personal information stored?

Our servers are located in the United Kingdom and the information that we collect directly from you will be stored in these servers.

Some of the organisations we share your personal information with (listed in section 3 of this policy) may be based or may make use of data storage facilities that are located outside the United Kingdom. Their handling and use of your personal information will involve us and / or them transferring it outside the United Kingdom. When we and / or they do this, we will ensure similar protection is afforded to it by:

- only transferring it or permitting its transfer to countries that have been deemed to provide an adequate level of protection for personal information under data protection laws; or
- using specific contracts with such organisations, which are approved for use in the United Kingdom, and which give your personal information the same protection it has in the United Kingdom after it is transferred.

Please contact our DPO for further information on the specific mechanism used by us when transferring your personal information outside the United Kingdom.

41. What rights do you have in relation to your personal information that we collect, hold and use?

It is important that the personal information that we collect, hold and use about you is accurate and current. Please keep us informed of any changes by contacting our DPO. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.
- Correction of any incomplete or inaccurate personal information that we hold and use about you.
- Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it.
- The transfer of your personal information to another organisation.

You can also object to us holding and using your personal information where our legal basis is a legitimate interest (either our legitimate interests or those of a third party).

Please contact our DPO if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

42. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to our DPO.

You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The Information Commissioner's website is https://ico.org.uk/ and complaints can be made here.

If you would like to receive this policy in alternative format, for example, audio, large print or braille, please contact our DPO.

43. Updates to this policy

We may update this policy at any time, and you should check this policy occasionally to ensure you are aware of the most recent version that will apply each time you access our website.

Last updated: January 2023