Title: **Data Protection - Group Procedure**

Business Function: **All Functions across Sanctuary Group**

Authors: **Legal Services**

Authorised by: **Group Director - Corporate Services**

Sanctuary Group:
Sanctuary Group is a trading name of Sanctuary Housing Association, an exempt charity, and all of its subsidiaries.

Uncontrolled copy if printed

CONTENT

General Information

1. Objective of this procedure

1.1 The objective of this procedure is to provide a framework to guide staff in the implementation of the Data Protection - Group Policy and to provide clarification on the data protection principles and what is meant by Personal Data.

1.2 It is vital that all staff involved in the managing and handling of Personal Data are appropriately trained as soon as possible upon commencement of their employment and supervised by the relevant Designated Officer on an ongoing basis. It is important that staff recognise that they as individuals are also responsible under the relevant data protection legislation including the Data Protection Act 2018 (the Act) and the General Data Protection Regulation (together, the Data Protection Law) and individual involvement in Data Breaches may result in disciplinary action.

1.3 This procedure should be read in conjunction with the following:

- Data Protection - Group Policy
- Archiving - Group Policy and Procedure
- Closed Circuit Television (CCTV) - Group Policy and Procedure
- Disciplinary - Group Procedure
- Freedom of Information - Sanctuary Scotland's Publication Scheme
- Homeworking - Group Procedure
- Acceptable Usage - Group Policy and Procedure
- Information Security - Group Policy and Management System Manual
- Content and Records Management - Group Policy and Procedure
- Tenancy Management - Housing Policy and Procedure.

2. Legislative/Regulatory context

2.1 References and sources are set out in the Data Protection - Group Policy. In particular, the policy and procedure are driven by the Group's obligations to comply with the regulatory and legal requirements of the:

- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679
- Privacy and Electronic Communications Regulations 2003

3. Responsibilities for implementation

3.1 Directors (or equivalent) are responsible for ensuring adoption of, and adherence to, this procedure and its associated policy relevant to their operation.

3.2 This procedure and its associated policy apply to all staff within the Group. All staff are responsible for reading and complying with this procedure and its associated policy, when dealing with Personal Data.

3.3 All staff will have a Designated Officer for data protection within their business area/region. The Designated Officer is responsible for promoting key data protection principles, ensuring staff comply with this procedure and its associated policy, and supporting staff with data protection queries. This includes regularly assessing within their business area/region:

- appropriate staff training;
- methods of handling and retaining personal information;
- requests from individuals to assert their data rights;
- Data Breaches; and
- staff performance when handling personal information.

3.4 The Data Protection team comprises the following functions (as appropriate):

- Data Protection Officer
- Legal Services
- Information Systems
- Human Resources
- Corporate Risk
- Insurance Services
- Communications.

3.5 The Data Protection team is responsible for investigating Data Breaches or suspected Data Breaches and taking any required action (or instructing operational teams to do so where appropriate), to ensure adequate safeguards are implemented to reduce the likelihood of similar breaches occurring again.

3.6 The Data Protection Officer is responsible for determining whether or not a Data Breach is reportable and, where it is a reportable Data Breach, reporting fully to the Information Commissioner's Office (ICO). The Data Protection Officer is also responsible for maintaining the Group's Registers of Data Breaches and Individual Rights Requests, and for monitoring compliance with the handling of such requests in accordance with the Data Protection Laws. The Data Protection Officer has direct access to the Group Board of Directors and reports directly into the Group Chief Executive on data protection matters.

3.7 All contractors and persons working on behalf of the Group must:

- ensure that they and all of their staff who have access to Personal Data held or processed on behalf of the Group, are aware of the data protection requirements and are fully trained in and are aware of their duties and responsibilities under the Data Protection Laws. This must be provided for in the written agreement between the Group and that individual/company. Any breach of the Data Protection Laws would therefore be a breach of that written agreement; and
- abide by the requirements of the Data Protection Laws with regard to Personal Data supplied by the Group.

4. What's new - What's different?

4.1 November 2020 - Formal review, no significant changes.

5. Definitions

5.1 The following definitions aim to support the user's understanding of this procedure.

Consent	Any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement for the Data Controller to process his or her Personal Data.
Data Breach	Any incident that results in the loss, alteration, unauthorised disclosure of, or access to, Personal Data for which the Group or a Group entity is a Data Controller or Data Processor. For the avoidance of doubt, any incident that results in the loss, alteration, unauthorised disclosure of, or access to, data that is not Personal Data does not fall within the scope of this procedure and its associated policy.
Data Processor	Any person (which can be a legal entity) who processes Personal Data on behalf of a Data Controller. The Data Processor may only process the data in accordance with the instructions of the Data Controller and cannot determine the purpose of processing itself. For example, the Group's Technology service providers, who may handle Personal Data on the Group's behalf, are likely to be Data Processors.
Data Controller	Any person (which can be a legal entity) who determines the purpose for which any Personal Data is to be processed. It is important that staff recognise that whilst the Group's Data Controller entities are responsible for compliance with the Data Protection Laws, staff may be liable for any breaches through disciplinary action.
Data Protection Impact Assessment (DPIA) Form	The form to assess any high risk data protection implications that might arise from: • the implementation of a new process; or • a change to an existing process. The form should be completed wherever changes are proposed, or a new process is proposed, and the process will involve high risk processing of Personal Data.
Data Subject	An individual who is the subject of Personal Data or Special Category Personal Data). This includes, but is not limited to, prospective, current or former residents, service users, employees, consultants and contractors.

Data Subject Access Request (DSAR)	A mechanism by which a Data Subject is entitled to request copies of, and information about, any of their Personal Data that is being processed by an organisation.
DSAR Form	The form to notify the business that a DSAR has been made, which must be completed and forwarded to Legal Services within one working day of receipt of the DSAR.
Designated Officer(s)	Staff member(s) with delegated responsibility for the implementation and day to day operation of the Group's data protection processes and procedures, including when dealing with DSARs and Data Breaches.
European Economic Area (EEA)	The European Economic Area.
Group	Any legal entity (i.e. asset owning subsidiary) that is part of the Sanctuary Group.
/nformation Commissioners Office (ICO)	The United Kingdom's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Personal Data	Information from which a living individual (the Data Subject) can be identified. This includes information such as telephone numbers, names, addresses, email address, photographs, CCTV footage, IP addresses and other unique identifiers, and voice recordings. It also includes personal opinions, for example a staff member may think that a service user is irate from their tone and record this opinion. The opinion is likely to be the Personal Data of both the member of staff and the service user.
Special Category Personal Data	Personal Data which relates to any of the following areas: • Racial or ethnic origin • Political opinions • Religious beliefs or philosophical beliefs • Trade union membership • Genetic data • Biometric data for the purpose of uniquely identifying a natural person • Health • Sex life or sexual orientation. Additional safeguards must be in place when processing Special Category Personal Data as well as data relating to criminal convictions and offences. Staff should contact Legal Services if they have queries regarding this. Special Category Personal Data is the new name for what was previously known as sensitive Personal Data under the Data Protection Act 1998.

Detailed Procedures

1. Data Protection overview

1.1 Data Controllers must comply with key principles of data protection. Those principles require that Personal Data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.1.1 Sections 1.2 to 1.9 provide more detail on these principles.

1.2 What is Personal Data?

1.2.1 Personal Data is defined as information from which a living individual can be identified (see Definitions table). In most instances, it is clear whether or not information is Personal Data but when in doubt, staff must refer to Legal Services.

1.3 How to ensure Personal Data is Processed Transparently - Privacy Statements.

1.3.1 To process Personal Data transparently, staff must make sure that they only process Personal Data where the Data Subject has been provided with a privacy statement which includes the information stipulated by Article 13 of the GDPR. That information includes (but is not limited to):

(a) the identity and contact details of the Data Controller;
(b) the contact details of the Data Protection Officer;

(c) the purpose for which the data is to be processed by the Group;
(d) the legal basis for the processing;
(e) where the legal basis for processing is a legitimate interest, a description of what that legitimate interest is;
(f) the identities of anyone to whom the data may be disclosed or transferred (if any); and
(g) confirmation of whether the Data Controller intends to transfer the Personal Data to another county (in which case seek advice from the Data Protection Officer in relation to additional information which needs to be provided to the Data Subject).

1.3.2 The privacy statement should be issued at the time of collecting the data either from the Data Subject or from a third party.

1.3.3 It is important that each time a new exercise is launched involving the collection of Personal Data or Special Category Personal Data from Data Subjects, a tailored privacy statement based on the Group's template privacy statement is drafted (see 2.3 below for further guidance).

1.3.4 Each privacy statement must be approved by the relevant Designated Officer before it is used. The Designated Officer shall keep a record of all approved privacy statements issued.

1.3.5 Personal Data may only be processed for the specific purposes for which it was collected except in very limited circumstances. This means that Personal Data must not be collected for one purpose and then used for another. Where it becomes necessary to change the purpose for which the Personal Data is processed, the Data Subject must be provided with a new privacy statement which sets out the prescribed information referred to above. If the Data Subject's consent to process their Personal Data is required, then a GDPR-compliant Consent must also be obtained.

1.4 How to ensure Personal Data is Processed Transparently - A Lawful Basis

1.4.1 To lawfully process Personal Data, the Group must rely on a lawful basis set out in the Data Protection Laws. One such lawful basis is where the Data Subject has provided their Consent. If Consent has not been provided, a different lawful basis for processing the Personal Data will need to be identified. See Tables A and B below which summarise the conditions for processing most relevant to the Group.

1.4.2 Where written Consent to the processing has not been obtained, or it is unclear as to whether it has been obtained previously, staff must make sure that any processing of Personal Data carried out meets at least one of the conditions in Table A and where the Personal Data is Special Category Personal Data, at least one of the conditions in Table B as well. However, the conditions in Table B for processing Special Category Personal Data are limited, so staff may find it easier to obtain the written Consent from the Data Subject where this is the case.

Table A (all Personal Data)

Legitimate Interests	The Group's legitimate business interests include, for example, the provision of social housing, supported and sheltered housing services, care, and management only services. The normal processing of Personal Data, which does not adversely affect an individual but is required in the day to day provision of these services, is permitted. Where there is a serious mismatch of competing interests between the Group and a Data Subject, the Data Subject's interests come first. Where there is any doubt as to whether there are competing interests, refer to the Data Protection Officer for advice.
Contracts	The use of a Data Subject's Personal Data in ways which are necessary in order for the Group to perform its services under the contract, or enforce its contractual rights, will be permitted.
Legal Obligations	To comply with legal obligations placed on the Group (other than contractual obligations considered above).
Vital Interests of Data Subject	To protect the Data Subject's vital interests (for example, in a life or death situation). This will only be a lawful basis for processing a Data Subject's Personal Data as a last resort and if it is not possible to obtain their Consent.

Table B (Special Category Personal Data only)

Explicit consent	Where the Data Subject has provided their explicit consent to the processing
Employment Obligations	To exercise the Group's legal obligations or rights in connection with employment, social security or social protection. This may include activities such as administering sick pay.
Legal Rights	To establish, exercise or defend the legal rights of the Group.
Health or Social Care	To provide health or social care or treatment, or to manage health or social care systems and services.
Vital Interests of Data Subject	To protect the Data Subject's vital interests (for example, in a life or death situation). Again, this only applies as a last resort.
Publicly Available Information	The Personal Data has been made public as a result of steps deliberately taken by the data subject.

1.5 How to ensure Personal Data is Processed Transparently - DPIAs

1.5.1 The Data Protection Laws now require organisations to carry out a DPIA for any data processing that is likely to result in a high risk to Data Subjects' rights and interests. A DPIA is a process designed to help the Group identify and analyse the data protection risks in a new project or process, so that steps can be taken to reduce these risks by appropriate planning and design.

1.5.2 Before implementing a new project or system or before making a change to an existing system, in each case that involves high risk data processing, staff should complete and submit a DPIA using the Group's DPIA Form. The Information Security team and the Data Protection Officer will then review the DPIA Form and make recommendations on how privacy should be protected in the new project or proposed change.

1.5.3 The DPIA Form must be completed for any project where data processing is likely to result in a high risk to individual rights. This might include projects or process changes which involve:

(a) Customer profiling and automated decision making, for example credit scoring individuals based on their financial history;
(b) Using Special Category Personal Data on a large scale, for example collecting health data about all housing applicants;
(c) Public monitoring, for example using CCTV in publically accessible areas;
(d) Matching data that has been collected from various sources;
(e) Processing biometric or genetic data, for example fingerprint identification;
(f) Using a newly developed technology that hasn't been tried and tested in the wider technology market.

1.5.4 In most cases it will be clear whether a DPIA Form should be completed for a new project or change to an existing process, but when in doubt, staff must refer to Legal Services.

1.6 How to ensure processing is adequate, relevant and limited to what is necessary

1.6.1 Before processing any Personal Data for a particular purpose, the Group needs to carefully consider what Personal Data is strictly necessary in order to achieve that purpose. If Personal Data is not necessary to achieve a specific purpose, it should not be collected.

1.6.2 As well as ensuring that any Personal Data obtained is necessary and relevant for the purpose for which it is being processed, staff must at the same time ensure they have adequate Personal Data to achieve the stated purpose. In other words, they must obtain enough data about an individual to enable them to perform their purpose(s) and no more.

1.7 How to ensure Personal Data is kept accurate and up to date

1.7.1 Personal Data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate. Staff must therefore take the appropriate steps to check the accuracy of any Personal Data at the point of collection and should verify the accuracy of Personal Data when interacting with Data Subjects (for example, when undertaking home visits or speaking with Data Subjects over the telephone).

1.7.2 Any Personal Data identified as inaccurate or out-of-date must be destroyed or erased from Group systems and, where required, replaced with current details. The Designated Officer in each office/department is responsible for ensuring Personal Data is kept accurate and up to date. See Section 4 (Data Retention) of this procedure for further guidance.

1.7.3 Although ultimately it is the Group's responsibility to make sure Personal Data is up to date and accurate, it is often reliant on the Data Subjects themselves to advise of any changes to their Personal Data. From a practical perspective staff should encourage Data Subjects to make contact with the Group when Personal Data becomes out-of-date or where they are aware of any inaccurate data the Group holds about them. The Group encourages Data Subjects to do this in its privacy statements. For further details on processes to assist with this obligation see Section 2 (Data Processing) of this procedure.

1.8 How to ensure Personal Data is not kept any longer than is necessary

1.8.1 Personal Data must not be kept longer than is necessary for the purpose(s) for which it was obtained. This means that Personal Data must be destroyed or erased from Group systems when it is no longer required for the purpose(s) for which it was collected. Personal Data must not be kept simply because it may become useful in the future for an unspecified purpose.

1.8.2 For guidance on how long data is likely to be kept before being securely destroyed, see Section 4 (Data Retention) of this procedure.

1.9 The rights of Data Subjects under the Data Protection Laws

1.9.1 Data Subjects are granted various rights by the Data Protection Laws, including:

(a) The right to ask to see what Personal Data the Group holds about them. This is known as a DSAR and the process for handling these requests is set out in Section 3 (Data Disclosure) of this procedure.
(b) The right to require the Group to rectify any Personal Data which is inaccurate. For example, where a Data Subject requests that their records are updated to reflect a change of address, staff must make those changes immediately. Where inaccurate Personal Data about a Data Subject has been legitimately passed on to a third party, it may also be necessary to correct the third party's data, depending on the nature of the data and whether the third party is still likely to be using it. Staff must keep a record of the change(s) made, the circumstances in which they were made and discuss it with their Designated Officer or the Data Protection Officer where necessary.

(c) The right to prevent processing of their Personal Data where this has caused or is likely to cause damage or distress. For example, where a joint tenant dies and upon being informed of this the Group either:
  (i) fails to update its records immediately; and/or
  (ii) continues to address correspondence in the names of both previous joint tenants.

(d) The right to erasure (also known as the right to be forgotten) which will typically apply where the Data Subject has withdrawn their Consent for the processing or where there is no longer a lawful basis for the Group continuing to process the information.

(e) The right to portability which entitles the Data Subject to receive the Personal Data which the Group holds on that Data Subject in a structured and commonly used and machine-readable format.

(f) The right to ask for the criteria involved in any automated decision taken without human input (i.e. by a computer), and for that decision to be reviewed. Again, staff must contact Legal Services when such a request is received.

(g) The right to prevent the Group sending unsolicited marketing materials to them.

1.9.2 When such a request is received, staff must discuss this with their Designated Officer immediately and complete the Group's Data Subject Rights Request form.

1.10 Security measures

1.10.1 All staff have a responsibility for ensuring Personal Data is kept secure at all times, so that there is no instance of unauthorised access, accidental loss/ destruction/damage, or theft of data from any location. This not only includes offices, but also staff members' homes or vehicles, and applies equally to members of staff who frequently work from home and those that undertake their work duties at home occasionally from time to time. Therefore, staff must be familiar with the Homeworking - Group Procedure. In addition, staff must follow Section 4 (Data Retention) of this procedure.

1.10.2 Staff must not disclose any Personal Data to a third party (i.e. a person or organisation who is not the Data Subject) unless they have informed the Data Subject in a privacy statement that their Personal Data may be disclosed to such parties (by name or by category). If the lawful basis for using that Personal Data is that the Data Subject has provided their Consent, then their Consent to the transfer will also need to be obtained. Any requests for Consent should meet the requirements of the Data Protection Laws (see Definitions Table for further information).

1.10.3 Any disclosure of Personal Data must be subject to appropriate security safeguards and, depending on the nature of the Personal Data, confidentiality obligations. For example, where Personal Data is being transferred in paper form to a contractor (subject to there being a lawful basis for the transfer, and the contractor complying with the Data Protection Laws), recorded delivery should generally be used rather than the ordinary post, and where electronic data is exchanged it may need to be encrypted.

1.11 Personal Data transfer outside of the EEA

1.11.1 Staff must not transfer Personal Data to a country outside of the EEA (which constitutes all of the European Commission Member States, Norway, Iceland and Liechtenstein; if in doubt, contact the Data Protection Officer) or share data with a third party who will do so unless:

(a) it is to perform a contract with the Data Subject;
(b) the Data Subject has provided their clear Consent;
(c) the country is on the ICO's approved countries list. Please contact the Data Protection Officer for details of approved countries; or
(d) a contract has been put in place with the third party/third parties to whom the Personal Data is to be transferred, based on certain European Commission approved standard contracts for transfers of Personal Data outside of the EEA. Please contact the Data Protection Officer when such a contract is required.

1.11.2 Please refer to Section 3 (Data Disclosure) of this procedure for further details.

1.12 Regulation and enforcement of the Data Protection Laws.

1.12.1 The ICO is the regulator of the Data Protection Laws. The responsibilities of the ICO include:

(a) promoting good practice and observance of the Data Protection Laws;
(b) spreading information on the Data Protection Laws;
(c) encouraging the development of codes;
(d) conducting assessments of Data Controllers at the request of Data Subjects;
(e) enforcing the Data Protection Laws (see below); and
(f) inspecting Data Controllers but only with the permission of the Data Controller (unless the Data Controller is a public body where the ICO does not need their permission).

1.12.2 When the ICO determines that the Data Protection Laws have been breached, the ICO can enforce one of the following four remedies:

(a) Seek an undertaking from the Data Controller to do/not to do certain things;
(b) issue an information notice requiring the Data Controller to provide certain information to the ICO;
(c) issue an enforcement notification with which the Data Controller must comply; or
(d) from May 2018, issue a fine of up to €20,000,000 (or 4 per cent of annual global turnover if higher).

1.12.3 Every member of staff within the Group is responsible for acting in accordance with the Data Protection Laws, and this procedure and associated policy. All Data Breaches are taken seriously and are likely to result in disciplinary action where appropriate. Staff must therefore be familiar with the Disciplinary - Group Procedure.

1.12.4 Where a member of staff suspects that a Data Breach has occurred, they must complete the Data Breach Reporting Form and notify their Designated Officer immediately. See **Appendix 1** - Data Breach - Investigating and Reporting Flowchart.

1.12.5 Where staff are unsure as to whether a Data Breach has occurred, they must still follow the process in paragraph 1.12.4 above so that a decision can be made by the Data Protection team as to whether a breach has occurred. The Data Breach Reporting Form should be completed and submitted to Legal Services for every Data Breach or suspected Data Breach that occurs.

2. Data processing

2.1 Purpose for data processing

2.1.1 Personal Data is only collected by the Group where it has a clear purpose to enable the Group to provide some aspect of its services or comply with legislation. The purpose for collection and processing must be clearly identified to the Data Subject in the privacy statement (see paragraph 2.3 below).

2.1.2 The Data Controller can be the Group, where the Group entity decides the purpose for which data is processed and dictates how data is treated. This is usually the case with Personal Data held by the Group and means that the Group entity takes on full liability for the accuracy, security, use of the data and for complying with the Data Protection Laws.

2.1.3 There may be circumstances where the Group entity is a Data Processor. This means it processes Personal Data on behalf of another organisation or collected by another organisation, which is the Data Controller. In these situations, the Group entity may only process the data in accordance with the Data Controller's instructions. The GDPR applies to Data Processors as well as Data Controllers.

2.2 Collecting Personal Data

2.2.1 Examples of the ways in which the Group collects data are:

(a) the Group's standard forms (for example, Tenancy Application Form, Home Ownership Application Form, Job Application Form);
(b) surveys;
(c) telephone conversations;
(d) emails; or
(e) home visits.

2.2.2 The Group telephone call recording system is the only approved method used for recording incoming and outgoing telephone calls and must only do so for regulated purposes. Sanctuary Group staff must not use equipment (such as Smartphones or Dictaphones) to record telephone or face to face conversations without authorisation and prior consent. The interception, recording and monitoring of telephone calls is governed by a number of different pieces of UK legislation which must be complied with (these are listed in the Data Protection - Group Policy).

2.2.3 The Lawful Business Practice (LBP) Regulations specify conditions upon which telephone calls may be recorded. These are to:

(a) provide evidence of a business transaction;
(b) ensure that a business complies with regulatory procedures;
(c) see that quality standards or targets are being met in the interests of national security;
(d) prevent or detect crime and investigate the unauthorised use of the telephone call recording system; and
(e) secure the effective operation of a telephone call recording system.

2.2.4 Recordings may also be used:

(a) for training purposes;
(b) to improve customer care;
(c) to support the investigations of complaints, particularly those concerning harassment at work;
(d) to support disciplinary work; and
(e) to provide evidence for the above regulatory legislation.

2.2.5 As already stated, Data Subjects have a right under the Data Protection Laws to request a DSAR and in response the Group must provide a copy of all Personal Data relating to that Data Subject held by the Group. It is therefore important that, in order to comply with its obligations under the Data Protection Laws, the Group is aware of where Personal Data is held and that such Personal Data is accessible. Personal Data should therefore not be created locally using unapproved and inaccessible mediums such as social media (for example Twitter or Facebook), text message or communications applications (for example WhatsApp).

2.2.6 When corresponding with a service user by email, steps should be taken to verify the identity of the service user before disclosing any Personal Data. For example, the service user's account should be checked to confirm whether the email address being used matches the email address registered on the account. If there is no email address registered on the account or the address on the account does not match, the service user should be contacted by telephone to verify that it is the service user making contact by email. Once this has been verified, the updated email address should be added to the Service User's account.

2.3 Subject notification when processing data

2.3.1 The Group's standard forms contain privacy statements that provide key information to Data Subjects about how their data is to be processed. The privacy statement is very important before any processing of Personal Data but particularly so where the Group is relying on the Data Subject's Consent.

2.3.2 There is a general privacy statement on the Group's website. Whilst staff may use this as a basis for a privacy statement when collecting information via the website, additional information must be included to ensure that the Data Subject has the information prescribed by the Data Protection Laws.

Note: Each privacy statement must be tailored to the circumstances in which the data is being collected. Legal Services can be consulted should a tailored privacy statement be required.

Note: The Group's template privacy statement is only for use where data is processed within the EEA. Where data collected may be processed outside the EEA, this template must not be used, and Legal Services should be contacted for assistance in preparing a suitable privacy statement.

Note: The website privacy statement must **not** be used or referred to in other non-web based documents because it is specific to information collected on the website. As such, it is not appropriate when collecting information on questionnaires or forms that are posted to tenants and users.

2.3.3 In general, a privacy statement must contain the details set out in paragraph 1.3.1 above. In addition, the statement should also include the following information where it is fair and transparent to do so:

(a) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
(c) where the processing is based on the Data Subject's Consent, the existence of the right to withdraw Consent at any time;
(d) the right to lodge a complaint with the ICO;
(e) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data; and
(f) the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2.3.4 All privacy statements must be approved by the Designated Officer before being used.

2.4 Appropriate data processing

2.4.1 Applicant and service user records: Staff must regularly ensure that data is correct and up-to-date - this can be achieved by numerous means including:

(a) recording the date that data is received;
(b) reviewing the applicant's details on a regular basis;
(c) checking information against other/previous sources, as applicable;
(d) requesting references from previous landlords where appropriate;
(e) comparing information on application forms with references, information on waiting list and written and verbal information from contacts with local authority, other agencies and other housing associations;

(f) checking housing benefit details with Local Authorities/the Department for Work and Pensions for rent purposes;
(g) undertaking six monthly reviews of waiting lists;
(h) amending details upon request of the service user;
(i) maintaining regular contact with support agencies;
(j) undertaking regular monitoring by maintaining data in line with home visits or, at any other point of interaction with Data Subjects; and
(k) taking time to talk to the service user by telephone or at home visit to check information when discrepancies are identified.

Note: Staff must take all reasonable steps to ensure data is accurately recorded, for example using a spell check tool.

2.4.2 Staff records: Staff must ensure that the data is correct and up to date by:

(a) recording the date that data is received;
(b) making sure the information that comes from the employee/consultant is signed;
(c) comparing with references gathered from current and previous employers;
(d) obtaining copies of certificates such as, drivers' licences, motor insurance and MOT certificates which must be updated annually;
(e) ensuring Staff Movement Advice (SMA) forms are completed for staff details;
(f) checking with personnel files and liaising with HR Services;
(g) checking against previous information where applicable;
(h) updating information upon request; and
(i) undertaking regular monitoring through periodic reviews and appraisals.

2.4.3 All staff must ensure that they make HR aware as soon as any of their personal details change.

2.5 Processing data outside the EEA

2.5.1 The Group may process data or give data to a Data Processor to process on its instructions anywhere within the EEA.

2.5.2 Where the Group wishes to process data outside the EEA, extra obligations apply. Consent may be required from Data Subjects to send their data outside the EEA.

2.5.3 When staff are asked to send data outside the EEA for any reason or they believe that this may happen, Legal Services must be consulted immediately and in good time before the data is sent.

3. Data disclosure

3.1 DSAR

3.1.1 Data Subjects can request to see all the Personal Data that the Group holds about them. The request can be made in any format, for example verbally or by email. The flowchart in **Appendix 2** summarises the process the Group adopts when a request like this is received; DSAR.

3.1.2 It is important that all staff follow these guidelines as failure to comply may put the Group and/or staff member in breach of the law. Where data is incorrectly disclosed, the Data Subject has the right, under the Data Protection Laws, to sue the Group. In addition, where data is not disclosed, and the Group has an obligation to do so, the Group may be subject to an order and/or fine from the ICO. In any event, the release of Personal Data must be authorised by a Designated Officer or in their absence, the Data Protection Officer before the Data is disclosed. If in any doubt, staff must contact their Designated Officer or the Data Protection Officer.

Remember: information cannot be recalled once it has been released.

3.1.3 Clarifications:

(a) A request for Personal Data may not always be obvious as Data Subjects do not have to quote the Data Protection Laws when requesting a copy of their Personal Data. If staff are unsure as to whether or not a request is meant to be a DSAR, they must discuss this with their Designated Officer promptly and before responding to the person in question. The only requirement for a DSAR is that it is in writing, although the Group does still treat DSARs received by telephone or other verbal communication as being valid.

(b) Staff may respond to the DSAR to seek further clarity of the request by asking for more details, verifying the requestor's identity, checking that the request is a DSAR or asking for a fee (where Legal Services has deemed that a fee is chargeable).

(c) Staff must verify the identity of the person requesting the information to be satisfied that they are the Data Subject. This may include obtaining and verifying against the Group's records:
(i) name;
(ii) address;
(iii) signature; and
(iv) organisation (as appropriate).

(d) As soon as a valid DSAR has been received, staff must complete the Group's DSAR Form. This form must be submitted within one working day of receipt of the request. Submitting the DSAR Form will trigger a notification of receipt of a DSAR to Legal Services, the relevant Designated Officer and the Technology department. The Designated Officer is responsible for managing the DSAR Form, and Legal Services are responsible for reporting on DSAR statistics and trends to the Group.

3.1.4 Timeframe

(a) The Group has one month from receiving a DSAR to provide the information to the applicant. The time to respond does not start until staff have all the details necessary to proceed with the request. Staff must meet this deadline as otherwise the applicant can make a complaint to the ICO. In the meantime, staff must acknowledge receipt of the request and, where chargeable, the fee, once received, and advise that all relevant information will be made available within the one-month limit.

(b) Where in limited circumstances staff are not able to meet the deadline, they must contact Legal Services and explain the reason for the delay, giving an estimate of when the information can be provided. In such cases, Legal Services will assess whether it would be reasonable to apply an extension to the deadline and, if so, the length of the extension to be applied. The extension will in no circumstances exceed two months.

3.1.5 Locate and compile information

(a) Staff must ensure that all media are searched for the information requested, for example, Personal Data held electronically, on paper files, in videos, photographs etc. This means that staff must perform a wide search for Personal Data held locally, although no more than is ‘reasonable’. There is no legal definition of ‘reasonable’ included in the Data Protection Laws. The Data Protection Officer can provide support in discussing with staff what the Group considers to comprise a reasonable search, as it may often depend on the specifics of the request.

(b) Staff must ensure that the DSAR Form is completed fully and accurately to allow the Technology department and/or the Hull DSAR team to carry out a targeted and timely search of the Group’s systems. As a general rule, the search terms for the IS systems search should be restricted to the Subject’s:
   (i) Full name (first name, last name); and
   (ii) First line of address.

(c) Staff should also indicate which folders in the S: and H: Drives it would be relevant to search, as it is not practical or reasonable for IS to search all folders across all locations and operations.

(d) Where Personal Data is held in a document containing other information only the relevant Personal Data should be extracted from the document. The document in its entirety must not be disclosed.

(e) Staff must ensure when disclosing data that they do not release any data which directly or indirectly reveals the identity of a third party or Personal Data relating to that third party. This does not mean that staff can refuse to release the data, it simply means that care must be taken to conceal the identity of any third party. For example, on paper documents, blacking out such sections of data alone may not obscure the content which potentially could be read if the paper document is held up to the light. The recommendation is that paper documents are redacted electronically (ensuring that redactions are finalised so that they cannot subsequently be undone) to produce the final version ready for disclosure.

Note: Whilst electronic disclosure is the preference, disclosure of information must be made in a format agreed with the requestor. Staff must always ensure that they send Personal Data securely, by special delivery or other secure mailing method and obtain proof of sending when posting or by password protected transmission when sending electronically.

3.1.6 Checklist

(a) What to send to the applicant?
  (i) a description of the Personal Data held;
  (ii) the purposes for which the data is processed;
  (iii) the recipients to whom the information is disclosed;
  (iv) the source of the data; and
  (v) any criteria used in extracting automated data (if applicable).

(b) The Designated Officer handling the request must update the relevant DSAR Form within two days of the DSAR being responded to so that the DSAR register can be maintained.

3.1.7 Withholding Personal Data

(a) There are very few exemptions in the Data Protection Laws which allow staff to withhold a Data Subject's Personal Data from them, as the law presumes that disclosure takes place. No 'value judgement' may be made about Personal Data to be disclosed and the data must never be edited or tampered with before disclosure, unless a valid exemption applies (for example, the protection of the identity of third parties).

(b) The following are the exemptions (situations in which data can be withheld from the Data Subject) which are most likely to apply to the Group. Advice from the Data Protection Officer can be sought where necessary before relying on one of the following:
  (i) data that is processed for the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or duty; in each case to the extent that disclosure to the Data Subject would be likely to prejudice those matters;
  (ii) data that also relates to another identifiable individual (a 'third party'), unless the third party has consented to their information being disclosed or it is otherwise reasonable to disclose the data without the third party's consent;

(iii) data that consists of information in which a claim to legal professional privilege could be maintained in legal proceedings; and
(iv) data that consists of a reference given in confidence for the purposes of the Data Subject's employment, training, education or service provision.

3.1.8 Requests by telephone

Some departments within the Group routinely answer queries from service users over the phone, giving out details of rent arrears or other details about their tenancy. Whilst some of this information is considered Personal Data, the service user's telephone request is not logged as a DSAR as the request is not made in writing and this service is offered to service users as part of their tenancy. Staff must follow the relevant local guidelines for conducting data protection checks before speaking to and disclosing Personal Data to service users over the phone.

3.2 Personal Data requested by a third party

3.2.1 In some instances, Personal Data may be requested from the Group by a person other than the Data Subject themselves. For example, by lawyers acting for their clients or by relatives of elderly service users.

3.2.2 Staff must never disclose Personal Data to a person other than the Data Subject unless the Data Subject has given their written consent to the Group to make a disclosure to another person and the original request for data was in writing. Both consent and request letters must be held on file.

3.2.3 Staff must also check whether there are any conditions attached to the consent, such as that it was only valid for a particular time or in specific circumstances.

3.2.4 Once staff are satisfied that the third party is making an approved DSAR on behalf of a Data Subject, then they must follow the steps outlined in Section 3.1 of this procedure.

3.2.5 In the absence of the written consent of the data subject, the DSAR must be declined.

3.3 Disclosing data to a third party at the Group's initiative

3.3.1 Sometimes the Group shares data about its employees and service users with third parties. For example, carers arranged by the Group for elderly or disabled tenants require a lot of information, some of it Special Category Personal Data, in order to do their jobs effectively.

3.3.2 Staff must never disclose Personal Data to a third party unless:

(a) the Data Subject has consented in writing or there is another lawful basis for sharing the Personal Data (for example, it is necessary for the Group to perform its contract with the Data Subject);
(b) the Data Subject has been informed of the data sharing through a privacy notice; and

(c) there is a written agreement in place with the third party which contains the minimum clauses required by the Data Protection Laws. See paragraph 3.4 for further details.

3.4 Disclosing to data processors

3.4.1 When Personal Data is disclosed to a third party, that third party may be a Data Processor (if they are processing the data on behalf of the Group). Not all third parties are Data Processors; some are Data Controllers in their own right.

3.4.2 The Group has obligations to ensure that its Data Processors adhere to the Data Protection Laws. Even when the Data Processor handles all Personal Data on behalf of the Group, any breaches of the Data Protection Laws are likely to impact the Group, so it is imperative that the following steps are adhered to:

(a) it is a legal requirement that there is a written agreement in place between the Group and its Data Processors (this will sometimes be the formal services contract between the Group and the Data Processor, and it will sometimes be a separate data sharing agreement); and
(b) the agreement must contain clauses prescribed in the Data Protection Laws such as requiring the Data Processor to only process the data in accordance with the Group's instructions, to keep the data secure and to ensure the integrity of staff with access to the data.

3.4.3 Staff must obtain authorisation from their Designated Officer before disclosing Personal Data to a third party to ensure that this agreement is in place. If in any doubt, contact Legal Services.

3.5 Freedom of Information

3.5.1 The Freedom of Information Act 2000 (FOIA) and the FOISA give individuals the right to access public records held by public authorities. Currently, the Group is not deemed to be a public authority in England and Wales as defined in the FOIA and accordingly is not governed by this Act.

3.5.2 With effect from 11 November 2019 Sanctuary Scotland Housing Association Limited and its subsidiaries (Sanctuary Scotland) now fall within the scope of the FOISA when carrying out regulated housing activities. Sanctuary Scotland's social housing activities are therefore subject to this Act, but the Group's care and student operations in Scotland are currently outside of its scope.

3.6 Therefore, if a request is made which is not a request for Personal Data, the request should be reviewed to assess whether it falls within the scope of the FOISA, and if so, the requestor should be directed to Sanctuary Scotland's Freedom of Information Request Form. The Group's FOISA team can support staff on making this assessment where required, as well as Legal Services.

3.7 If the request does not fall within the scope of the FOISA, the request can be declined unless the Group is comfortable disclosing the information voluntarily.

4. Data retention

Note: Section 4 does not give information on how long every type of Personal Data can be retained. The overriding requirement is that when the purpose for which Personal Data was collected has come to an end, that Personal Data should be returned to the Data Subject or deleted (as appropriate). Personal Data must not be archived unless there is a specific and identified purpose for archiving the Personal Data of which the Data Subject is aware and for which the Group has a lawful basis.

Note: Staff must consider whether there are any data retention practices and procedures, specific to their department, which they must also comply with. Staff must make decisions about how long to keep certain Personal Data on a case by case basis. Where staff are unsure about whether certain Personal Data can be retained, they must refer to their Designated Officer or the Data Protection Officer.

Phase	Action
Retention of relevant data	All offices must ensure that each file is reviewed to check the accuracy of any Personal Data captured: • at the point of collection; • updated in line with home visits; or • at any other point of interaction with data subjects. The purpose of this action is to destroy unnecessary documents and/or summarise information where possible and that data in only retained for the appropriate length of time in accordance with the Content and Records Management - Group Policy and Procedure.
Secure retention of relevant data	All offices must ensure that only authorised staff have access to the data and that the data remains safe, intact and complete.
Archiving data	All offices must ensure that: • only necessary data is archived; and • the data must be stored via the appropriate media to ensure its preservation for the length of time it is required.
Maintaining the Data Subject's accessibility	All offices must ensure that the data remains available to the Data Subject by filing the data in an appropriate filing system.
Data destruction	All offices must ensure that inappropriate data and data with expired retention periods are destroyed securely.

4.1 Data retention definition

4.1.1 Data retention covers:

(a) ensuring Personal Data is accurate, up-to-date and remains relevant whilst it is stored. This requires regular reviews and responding to input from Data Subjects;

(b) security of data (day-to-day, in the longer term and when in transit);
(c) the period of retention which must be only as long as is necessary or as dictated by law; and
(d) destruction of data in a secure manner once data is no longer needed.

4.2 Review of records

4.2.1 Review of service user records - files holding information about service users must be reviewed at every appropriate opportunity. Such reviews include:

(a) change of circumstances notification (for example, marital status, children, job, etc.);
(b) status on waiting lists and related paperwork;
(c) six-monthly review of data on service user applicants and related paperwork;
(d) more regular reviews of information on current service users may be established by individual offices/departments;
(e) for former service users, reviews must be carried out when the tenancy is terminated and subsequently, at least every three years until the data has been destroyed.

4.2.2 Review of staff records - files holding information on prospective, current or former employees and consultants must be reviewed regularly. Such reviews include:

(a) notification of change of circumstances (for example, address, marital status etc.);
(b) six monthly review of data on job applicants;
(c) annual review of data on current employees and consultants;
(d) for former employees and consultants, all offices review data;

(e) when the employee/consultant ceases to work for the Group; and
(f) subsequently, at least every three years until the data has been destroyed.

4.2.3 Review of contractors'/cleaners' records - files holding information on the contractors/cleaners working for the Group must be reviewed annually.

4.3 Security

4.3.1 Data security - at all times, all staff must ensure Personal Data (including Special Category Personal Data) is stored securely.

4.3.2 Only staff who have a need to access information about service users or other staff may do so. Personal Data and Special Category Personal Data must be stored securely as follows:

(a) for data in hardcopy form, the data must be locked away in a cabinet when not in use and at the end of every day. Keys must be stored securely;
(b) for data on microfilm, the data must be locked away. Keys must be stored securely; and

(c) for electronic data, the data must be kept on files only accessible with the user login and password of authorised staff, who have to comply with security measures as indicated in the Information Security - Group Policy and Information Security Management System Manual and also the Acceptable Usage - Group Policy and Procedure.

4.3.3 Data environment - staff must ensure that data is stored on the appropriate media given its expected lifecycle period:

(a) files on local PCs, laptops or USB drives must be backed up with master versions stored on H: (Home) or S: (Shared) network drives;
(b) thermo paper expires after approximately one year;
(c) CD-ROMs after 10 years; and
(d) conventional paper is permanent when stored appropriately.

4.3.4 To ensure that data is not lost or damaged during storage, the storage space must be dry, and the data must be kept in the dark at normal room temperatures.

4.3.5 For archiving, storage must be either on the Group's premises or in spaces designated by the Group. Refer to Archiving - Group Policy and Procedure.

4.3.6 Data in transit - Where data needs to be taken off-site, staff must ensure it remains secure and kept with them at all times. Staff must never leave Personal Data unattended.

4.3.7 All mobile devices used to access Personal Data (for example laptops, USBs, smart phones) must be encrypted and password secured. For further details contact the Technology department.

4.3.8 Data in hard copy must be in a locked document carrier with the key securely stored. Staff who are homeworkers, or who work at home from time to time, must also refer to and comply with the Homeworking - Group Procedure.

4.3.9 Each office must implement a 'check out' system when data needs to be taken off the premises where it is normally stored. The Designated Officer is responsible for the maintenance of this system, which must record the date(s) and the name of the person who is removing and/or returning the data.

4.4 Retention period

4.4.1 Personal Data may only be retained for as long as it is necessary for the purpose for which it was collected. This means data must be constantly assessed to determine whether it is still relevant or whether it is to be deleted/destroyed. The Content and Records Management - Group Policy and Procedure includes a retention schedule setting maximum retention periods after which categories of data must be destroyed in the absence of exceptional circumstances, for example, ongoing litigation. However, the records management retention schedule is only for guidance and staff must always consider whether Personal Data must be deleted sooner in order to comply with the Data Protection Laws.

4.5 Archiving data

4.5.1 Data may be archived when access is no longer required day-to-day. However, archived data is still subject to the Data Protection Laws. Archiving applies to both relevant original and summarised information.

4.5.2 Service user records - authorised staff can archive data on former service users. Any Personal Data (including Special Category Personal Data) collected during the resident's application and/or during the service user's tenancy with the Group is to be reviewed regularly. Authorised staff must only retain relevant documents and data. However, generally these are not archived as they are current or open files.

4.5.3 Employee records - Authorised staff can archive data on former employees. Any Personal Data (including Special Category Personal Data) collected during the job application and/or during the employee's employment with the Group is to be reviewed for updating and authorised staff only retain relevant documents. However, generally these must not be archived as they are current or open files

4.5.4 Contractors'/cleaners' records - Contractors'/cleaners' records containing Personal and Special Category Personal Data about individuals are generally current or open files and are therefore unlikely to be archived.

4.6 Categories of waste and data destruction

4.6.1 Deleting/destroying unnecessary data includes:

(a) original documents, which are not to be retained by law;
(b) files on local PCs, laptops or USB drives must be backed up with master versions stored on H: (Home) or S: (Shared) network drives;
(c) unnecessary information;
(d) outdated/expired information; and
(e) inappropriate information.

4.6.2 Unnecessary, inappropriate, outdated information and/or expired data about data subjects must be destroyed securely by:

(a) cross cut shredding for paper documents and microfibre;
(b) confidential waste disposal for floppy disks, memory sticks, CD-ROMs and other removable media;
(c) deleting electronically for soft copy material; or
(d) laptops must be returned by hand or secure courier to the Technology department for secure decommissioning.