**Title:** **Data Protection - Group Procedure**

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

**Authors:** **Data Protection Team**

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

# CONTENT

# General Information

## 1. Objective of this procedure

1.1 The objective of this procedure is to provide a framework to guide Sanctuary Group (Group) staff in the implementation of the Data Protection (DP) - Group Policy, provide clarification on what constitutes personal data, rights available to individuals, the DP principles, and how these should be applied to achieve compliance with the legislation, as well as and what is meant by personal data.

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

- Data Protection - Group Policy
- Archiving - Group Policy and Procedure
- Disciplinary - Group Procedure
- 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.
- Video Surveillance Management Systems (VSMS) - Group Policy and Procedure
- Inclusion for All - Equality, Diversity and Inclusion Strategy 2024 - 2026

## 2. Legislative/Regulatory context

2.1 References and sources are set out in the DP - Group Policy. This procedure is driven by the Group's obligations to comply with the regulatory and legal requirements of the:

- Data Protection Act 2018 (DPA 18)
- United Kingdom General Data Protection Regulation (UK GDPR)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

## 3. Responsibilities for implementation

3.1 Directors (or equivalent) are responsible for ensuring adoption of and adherence to this procedure.

3.2 Managers are responsible for applying this procedure and ensuring all their staff comply.

3.3 All staff are responsible for reading and complying with this procedure, appendices and its associated policy, when dealing with personal data.

3.4 Data Owners are responsible for the data within their domain and ensuring that it is governed throughout the organisation and in compliance with DP regulations.

3.5 Designated Officers (DOs) are responsible for the daily management of data within their area and support operational regulatory compliance with DP legislation.

3.6 The DP team is responsible for providing assurance to Executive about the Group's compliance with DP legislation, setting the Group's DP Work Programme and providing advice and guidance to staff.

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

4.1 May 2024 - Formal review, significant updates made to reflect implementation of new DP team and associated updated processes. New appendices added:

- **Appendix 1** - Data Subject Access Request - Group Process
- **Appendix 1A** - Data Subject Access Request - Group Process Flowchart
- **Appendix 2** - Data Subject Rights Request - Group Process
- **Appendix 2A** - Data Subject Rights Request - Group Process Flowchart
- **Appendix 3** - Data Breach - Group Process
- **Appendix 3A** - Data Breach - Group Process Flowchart
- **Appendix 4** - Data Protection Impact Assessment - Group Process
- **Appendix 5** - Marketing - Group Process
- **Appendix 6** - Designated Officer Role and Responsibilities
- **Appendix 7** - Data Owner Role and Responsibilities

## 5. Definitions

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

| | |
|---|---|
| ***Anonymisation*** | Anonymous information is information which does not relate to an identifiable person or has been modified in such a manner that the Data Subject is no longer identifiable. Anonymisation is different from pseudonymised data as outlined below. |
| ***Caldicott Guardian*** | Is a senior person responsible for overseeing the confidentiality of care information and making sure it is used appropriately. |
| ***Consent*** | Consent is one of the six lawful bases for processing personal data under the UK GDPR. Consent is defined as a clear, specific, and freely given indication of an individual's agreement to the processing of their personal data for a specific purpose. |
| ***Data Breach*** | Any incident that results in the loss, alteration, unauthorised disclosure of, or access to personal data. |
| ***Data Processor*** | Any person or legal entity that processes personal data on behalf of a Data Controller.<br>A Data Processor may only process personal data in accordance with the written instructions of the Data Controller and cannot determine the purpose of processing. |

| | |
|---|---|
| ***Data Controller*** | A Data Controller can be a person or a legal entity that determines the means (how) and purpose (why) for which any personal data is to be processed and associated compliance responsibilities. In relation to this procedure, the Group will be the Data Controller. |
| ***Designated Officer (DO)*** | The DO(s) within a business area responsible for supporting operational DP compliance including the facilitation of individual rights requests.<br>The Group's list of DOs can be found on Solis. |
| ***Data Owner*** | The Designated Person(s) responsible for the data within their business area.<br>The Group's list of Data Owners can be found on Solis. |
| ***Data Governance Forum*** | Forum to discuss and govern data related matters across the Group attended by Data Owners. |
| ***Data Protection Impact Assessment (DPIA)*** | A DPIA is a process designed to help systematically analyse, identify, and minimise the DP risks of a project or change in processing. |
| ***Data Subject*** | An individual who is the subject of personal or special category data. This includes, but is not limited to, prospective, current or former residents, service users, employees, consultants and contractors. |
| ***Data Subject Access Request (DSAR)*** | Right of access - which enables a Data Subject is to request copies of, and information about, any of their Personal Data that is being processed by the Group. |
| ***Information Commissioners Office (ICO)*** | The ICO is the UK's independent body set up to uphold information rights and has enforcement and regulatory powers. |
| ***Mixed Data*** | Is personal information about an individual that also includes information about or is the personal data of another individual. |
| ***Personal Data*** | Information that relates to a living individual (Data Subject) from which they can be identified directly or indirectly in-conjunction with other information.<br>For example, Name, telephone numbers, addresses, email address, photographs, CCTV footage, audio recordings, IP addresses, SAP BP Number, and other unique identifiers, and voice recordings.<br>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 (mixed data). |
| ***Pseudonymisation*** | Pseudonymisation refers to techniques that replace, remove or transform information that identifies individuals, and keeps that information separate. Data that has undergone pseudonymisation remains personal data but is a tool that can help improve security and privacy of data. |

| | |
|---|---|
| ***Records of Processing Activity (RoPA)*** | A RoPA is an internal document that records all the processing activities undertaken by an organisation which involve the use of personal data. |
| ***Sanctuary Group (the Group)*** | Any legal entity (i.e. asset owning subsidiary) that is part of the Group. |
| ***Special Category Personal Data*** | Personal data which relates to any of the following areas:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious beliefs or philosophical beliefs<br>• Trade union membership<br>• Genetic data<br>• Biometric data for the purpose of uniquely identifying a natural person<br>• Health<br>• Sex life or sexual orientation. |
| ***Third Party with Authority*** | An individual who has written authority (been granted permission) to act on behalf of another person and/or access that individual's personal data. |

# Detailed Procedures

## 1. Data Protection Overview

1.1 What is Personal Data?

1.1.1 The UK GDPR states that, for information to be personal data, it must relate to a living person who is identifiable from that information directly or indirectly where other information can be combined to identify an individual.

1.1.2 What identifies an individual could be as simple as a name or a number, for example a BP Reference in SAP, Employee ID number. There will also be many other types of identifiers such as an IP address, location data, or a cookie identifier.

1.1.3 The context in which we hold information, and the way we use it, can have a bearing on whether it relates to an individual and therefore if it is the individual's personal data:

- **Example - Personal Data**:
  - Joe, lives at 123 Example Road. Joe emails into the Group to complain that his boiler is not working and requests a technician visits his property to inspect the boiler and repair it. Joe includes his address and contact details in the email.
  - In this scenario the information contained in Joe's email would constitute their personal data as they have expressed their opinion as well as provided details of where they live as well as their contact details.
- **Example - Not Personal Data**:
  - Joe lives at 123 Example Road. The Group holds compliance certificates for the boiler fitted at Joe's property. These certificates include the address details of where the boiler is fitted.
  - Although these certificates include Joe's address, they do not constitute Joe's personal data as they do not identify or relate to Joe as an individual but relate to an asset.

1.2 What is Special Category Data?

1.2.1 Special category data refers to specific types of personal information that are considered particularly sensitive and have additional requirements which must be met before they can be processed, which give them extra protection under DP laws.

1.2.2 Special category data is defined as personal data which relates to any of the following areas:

i Racial or ethnic origin
ii Political opinions
iii Religious beliefs or philosophical beliefs
iv Trade union membership
v Genetic data

vi Biometric data for the purpose of uniquely identifying a natural person
vii Health
viii Sex life or sexual orientation.

1.3 Data Controllers

1.3.1 Under the UK GDPR, a Data Controller is an entity or organisation that determines the purposes and means of processing personal data and exercise overall control of personal data.

1.3.2 A Data Controller is responsible for ensuring compliance with all the DP principes in the UK GDPR and has the ultimate responsibility for the protection and lawful processing of personal data. They are also responsible for the compliance of their Data Processor(s).

1.3.3 The Group will act as a Data Controller for the services it provides; however, there maybe instances when the Group also acts as a Data Processor on specific written instructions of another Data Controller.

1.4 Data Processors

1.4.1 Data Processors act on behalf of, and only on the written instructions of a Data Controller.

1.4.2 There may be circumstances where a Group entity is acting as a Data Processor. This means it processes personal data on behalf of 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 written instructions. The UK GDPR applies to Data Processors, as well as Data Controllers.

1.4.3 For the avoidance of doubt, Group employees are not considered Data Processors, as they act on the Group's direct behalf. External contractors or consultants for example who are contracted as a separate legal entity would be a Data Processor.

1.5 Information Commissioner's Office

1.5.1 The ICO is the regulator of the DP laws. The responsibilities of the ICO include:

(a) promoting good practice and observance of the DP laws;
(b) spreading information on the DP laws;
(c) encouraging the development of codes;
(d) conducting assessments of Data Controllers at the request of Data Subjects;
(e) enforcing the DP 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 its permission).

1.5.2 When the ICO determines that the DP 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 actions.
(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.
(d) Issue a fine of up to £17.5 million (or four per cent of annual global turnover if higher).

## 2. Staff Conduct and Requirements

2.1 Every member of staff within the Group is responsible for acting in accordance with the DP laws, this procedure, appendices, and associated policy. All breaches of DP laws are taken seriously and could result in disciplinary action where appropriate. Staff must therefore be familiar with the Disciplinary - Group Procedure.

2.2 All staff involved in the managing and handling of personal data should be appropriately trained as soon as possible upon commencement of their employment, and undertake appropriate refresher training every two years.

2.3 It is important that staff recognise that they as individuals are also responsible under the DP Act 2018, which outlines at section 170 that it is an offence for a person to knowingly or recklessly disclose, sell or procure information for disclosure.

2.4 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. 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 several different pieces of UK legislation which must be complied with (these are listed in the DP - Group Policy).

2.5 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.

2.6 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.

## 3. Contractors

3.1 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 DP requirements and are fully trained in and are aware of their duties and responsibilities under the DP laws.

3.2 This must be provided for in the written agreement between the Group and that individual/company. Any breach of the DP laws would therefore be a breach of that written agreement; and abide by the requirements of the DP laws with regard to personal data supplied by the Group.

## 4. Data Processing

4.1 DP Principles

4.1.1 The UK GDPR sets out seven key principles for the lawful processing of personal data, which lie at the heart of the general DP regime. These principles summarise what the law intends to achieve and must be abided by the Group and followed by all staff members for any activities that involve the processing of personal data. Those principles are:

(a) **Lawfulness, fairness and transparency**: personal data shall be processed lawfully, fairly, and in a transparent manner in relation to individuals.
(b) **Purpose limitation**: personal data shall be 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.
(c) **Data minimisation**: personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
(d) **Accuracy**: personal data shall be 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.

(e) **Storage limitation**: 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 UK GDPR in order to safeguard the rights and freedoms of individuals.

(f) **Integrity and confidentiality (security)**: personal data shall be 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.

(g) **Accountability**: organisations must have appropriate measures and records in place as proof of compliance with the data processing principles. Examples include the Group's Records of Processing Activities, Retention Schedule, DPIAs.

4.2 Lawful and Fair - Basis for Processing

4.2.1 To lawfully process personal data, the Group must identify an appropriate lawful basis as set out in the DP laws prior to collection and processing of personal data. Table A below outlines the lawful bases which can be relied upon.

4.2.2 When processing special category data, the Group must also identify an appropriate condition for processing and where required by the DPA 18 an appropriate basis in law. Table B below outlines the conditions for processing special category data and associated basis in law.

| **Table A (all Personal Data)** | |
|---|---|
| ***Article*** | **Description** |
| ***Article 6(1)(a) - Consent*** | The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes. |
| ***Article 6(1)(b) - Performance of Contract*** | Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract. |
| ***Article 6(1)(c) - Compliance with a legal obligation*** | Processing is necessary for compliance with a legal obligation to which the controller is subject. |
| ***Article 6(1)(d) - Vital Interests*** | Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person. |
| ***Article 6(1)(e) - Performance of a Task in the Public Interest*** | Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. |

| Table A (all Personal Data) | |
|---|---|
| ***Article*** | **Description** |
| ***Article 6(1)(f) - Legitimate Interests*** | Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child. |

| Table B (Special Category Personal Data only) | | |
|---|---|---|
| ***Article*** | **Description** | **DPA 18 - basis in law (Schedule 1 Conditions)** |
| ***Article 9(1)(a) - Explicit Consent*** | Where the Data Subject has provided their explicit consent to the processing for a specific purpose. | N/A |
| ***Article 9(1)(b) - Employment, Social Security and Social Protection Obligations*** | To exercise the Group's legal obligations or rights in connection with employment, social security or social protection.<br>This may include activities such as administering sick pay. | Condition 1 |
| ***Article 9(1)(c) - Vital Interests*** | To protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent | N/A |
| ***Article 9(1)(d) - Not-for-Profit Bodies*** | Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the Data Subjects. | N/A |
| ***Article 9(1)(e) - Made Public by the Data Subject*** | Processing relates to personal data which are manifestly made public by the Data Subject | N/A |
| ***Article 9(1)(f) - Legal Claims or Judicial Acts*** | To establish, exercise or defend the legal rights of the Group. | N/A |
| ***Article 9(1)(g) - Reasons of*** | Processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued and provide suitable specific measures to safeguard the | One of conditions 6 - 28 |

| Table B (Special Category Personal Data only) | | |
|---|---|---|
| ***Article*** | **Description** | **DPA 18 - basis in law (Schedule 1 Conditions)** |
| ***substantial Public Interest*** | fundamental rights and the interests of the Data Subject. | |
| ***Article 9(1)(h) - Health or Social Care*** | To provide health or social care or treatment, or to manage health or social care systems and services. | Condition 2 |
| ***Article 9(1)(i) - Public Health*** | The processing is necessary to protect against serious risks to health. | Condition 3 |
| ***Article 9(1)(j) - Archiving, Research and Statistics*** | The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. | Condition 4 |

4.2.3 Any processing of personal data by the Group must also be fair in that personal data should only be used in ways that people would reasonably expect and not in ways which would have an unjustified adverse effect on them. Each processing activity should be considered on a case-by-case basis.

4.2.4 For clarity this does not mean that personal data cannot be used in a way that negatively impacts individuals so long as it is justified. For example, we may process personal data to recover unpaid rent. From the individual affected perspective, this would have a negative impact on them but would be justified and therefore fair.

4.3 Transparency - Privacy Statements

4.3.1 The Group's processing of personal data must also be transparent to Data Subjects to enable them to exercise choice about whether they wish to enter into a relationship with the Group and provide their personal data.

4.3.2 To achieve transparency the Group must make available privacy statements that outlines the following information:

(a) name and contact details of our organisation - so individuals know who we are and how to contact us;
(b) contact details of the DP Officer;
(c) purpose for which the data is to be processed by the Group;
(d) the lawful basis for the processing, including the condition for processing and basis in law if processing special category data;
(e) rights available to individuals in respecting of the processing;
(f) retention period the data will be retained for following processing;
(g) right to lodge a complaint with the ICO;
(h) where the legal basis for processing is legitimate interests, a description of what that legitimate interest is;

(i) details of whether individuals are under a statutory or contractual obligation to provide their personal data and what the implications will be if they do not provide that data; and
(j) details of the existence of automated decision-making, including profiling.

4.3.3 The required privacy information outlined above must be available to Data Subjects prior to or at the point of collection of their data. This can be achieved via sign posting to the Group's website, which each Group privacy statement should be published to.

4.3.4 Privacy information can also be provided via other mechanisms such as in hard copy paper format or orally as appropriate depending on the nature and circumstances of the processing.

4.3.5 When the Group obtains personal data from a source other than the individual it relates to, the Group must provide the individual with the above privacy information outlined at 4.3.2:

(a) within a reasonable period of obtaining the personal data and no later than one month from receipt; or
(b) if the Group uses the data to communicate with the individual, at the latest, when the first communication takes place; or
(c) if the Group envisages disclosure to someone else, at the latest, when the Group discloses the data.
(d) if the Group plans to use personal data for any new purposes, we must update our privacy statement and proactively bring any changes to people's attention.

4.3.6 It is important that whenever a new processing activity is to be commenced, that there is an associated privacy statement in place prior to collection of personal or special category data from Data Subjects.

4.3.7 The Group has a corporate privacy statement template, that includes all required fields and that can be tailored to the specific processing activities taking place which is available from Solis.

4.3.8 Service areas are responsible for ensuring their privacy statements are accurate and compliant, with the DP team providing technical support to help achieve this. DOs support this process by highlighting the requirements within their business area, as well as informing the DP team of any changes to processing activities as and when they occur. This enables any required amendments to be made and documented to evidence the Group's compliance.

4.3.9 The DP team hold the Group's central register of privacy statements.

## 4.4 Purpose Limitation

4.4.1 The Group must only collect, and process personal data for specified, explicit and legitimate purposes, that 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 a privacy statement.

4.4.2 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.

4.4.3 Personal data can only be used for a new purpose, in the following circumstances:

(a) the Group has obtained the individual's specific consent for the new purpose;
(b) there is a legal or regulatory obligation requiring or allowing the new processing in the public interest;
(c) the new purpose is compatible with the original.

4.4.4 DP legislation outlines that when using data for statistical purposes it is considered compatible with the original purpose it was collected for. For all other purposes a compatibility assessment must be completed and documented to establish if the new purpose is compatible with the original.

4.4.5 A compatibility assessment must take into consideration the following:

(a) any link between the original purpose and the new purpose;
(b) the context in which the Group originally collected the personal data, specifically the relationship with the individual and what they would reasonably expect;
(c) the nature of the personal data and whether any is of a sensitive nature;
(d) possible consequences for individuals of the proposed new processing;
(e) Safeguards that can be implemented, for example encryption or pseudonymisation.

4.4.6 As a principle if the new purpose is either very different from the original purpose, would be unexpected or would have an unjustified impact on individuals, then it is highly unlikely to be compatible with the original purpose.

4.4.7 For support on conducting a compatibility assessment, please contact the DP team - dataprotetion@sanctuary.co.uk.

## 4.5 Data minimisation

4.5.1 The Group must ensure that the personal data processed is adequate (sufficient to properly fulfil our stated purpose), relevant (have a rational link to the purpose) and limited to what is necessary (so we do not hold more information or collect more categories of data than is needed for that purpose).

4.5.2 Before processing any personal data for a particular purpose, the Group should carefully consider what personal data is strictly necessary in order to achieve that purpose. If personal data is not necessary, it should not be collected. The Group should never collect information just in case.

4.5.3 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 summary, the Group must obtain enough data about an individual to enable us to perform the purpose(s) and no more.

4.6 Accuracy

4.6.1 All reasonable steps must be taken by the Group to ensure the personal data collected and held by the Group is accurate and kept up to date in the context of the processing. 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).

4.6.2 Any personal data identified as inaccurate or out-of-date must be updated, destroyed, or erased from Group systems as appropriate depending on the nature and purpose of the processing. DOs support this process within their area, but all staff have a responsibility for ensuring personal data is kept accurate and up to date.

4.6.3 Whenever possible staff should validate the accuracy of data when engaging with customers as part of routine service delivery as well as to encourage Data Subjects to notify the Group whenever personal data becomes out of date, for example contact details or changes in personal circumstances.

4.6.4 In relation to staff records, all staff must ensure that they keep their personal details up to date on the Group's HR system or make People Services aware as soon as any of their personal details change if they are unable to update them, themselves.

4.7 Storage Limitation

4.7.1 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.

4.7.2 Personal data must not be kept because it may become useful in the future for an unspecified purpose. If personal data is retained for longer than it is required for, the Group will no longer have a valid lawful basis for processing.

4.7.3 For guidance on retention please see Section 9.

## 4.8 Integrity and Confidentiality (Security)

4.8.1 The Group must implement appropriate technical and organisational measures to ensure the security of personal data and minimise the risk of any loss of confidentiality, integrity and availability.

4.8.2 All staff have a responsibility for ensuring personal data is kept and stored securely 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.

4.8.3 Staff must not disclose personal data to a third party (i.e. a person or organisation who is not the Data Subject) that do not have authority to access the information. If staff are in doubt about whether it is appropriate to disclose personal data, please seek advice from the DP team - dataprotection@sanctuary.co.uk.

4.8.4 Only staff who have a business 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 within Group systems, accessible with a network user login and password of authorised staff. For further guidance please see the Acceptable Usage - Group Policy and Procedure, Information Security - Group Policy, Information Security Management System Manual.

4.8.5 When disclosing personal data, this 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 DP laws), recorded delivery should be used rather than the ordinary post, and where electronic data is exchanged it should be shared via a secure encrypted mechanism.

4.8.6 Where data needs to be taken off-site, staff must ensure it remains secure and kept with them at all times and returned safely. Staff must never leave personal data unattended.

4.8.7 All Group issued mobile devices used to access personal data (for example laptops, smart phones) must be encrypted and password secured.

4.8.8 Personal devices maybe used to access Group provided apps, such as Office 365, SuccessFactors, and Kronos for example, in line with the following requirements:

(a) the device must use a supported operating system and must not be jailbroken or rooted,
(b) staff must not leave themselves signed in to any Group apps if you share the device, for example with family members or to allow children to play games on it,
(c) staff must report that the device has been lost or stolen to Technology as soon as they become aware of this.

4.8.9 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.

4.8.10 Technology, in partnership with the DP team, are responsible for leading on the implementation of appropriate technical and organisational security measures to protect the confidentiality and security of personal data. All staff must be familiar with and comply with the requirements of the Acceptable Usage - Group Policy and Procedure, Information Security - Group Policy, Information Security Management System Manual, Homeworking - Group Procedure.

4.9 Accountability

4.9.1 To meet the accountability principle, the Group must not just comply with the DP legislation but be able to demonstrate compliance. This is achieved through several mechanisms including for example documented policies and procedures, the Groups' Records of Processing Activities, Privacy Statements, and DPIAs.

4.9.2 The Group also has a statutory duty to embed DP by 'design and default'. This requires the consideration and implementation of the DP principles, as well as how Data Subject's right can be met and facilitated in relation to all of the Group's processing, processes, and procedures.

## 5. Data Subject Rights

5.1 DP legislation grants individuals various rights over their personal data. These are summarised below:

i. ***The right to be informed***: gives individuals the right to be informed about the collection and use of their personal data. The Group meets this right through providing privacy statements and making them accessible through the Group's websites and other mechanisms.
ii. ***The right of access***: to receive a copy of their personal data the Group holds about them and other supplementary information. This is known as a DSAR.
iii. ***The right to rectification***: to have inaccurate personal data rectified, or completed if it is incomplete. This right is not absolute and in certain circumstances the Group can refuse a rectification request.

iv. ***The right to erasure (also known as the right to be forgotten)***: gives individuals the right to have their personal data erased. This right is not absolute and in certain circumstances the Group can refuse an erasure request.

v. ***The right to restrict processing***: to restrict the processing of their personal data. For example, the Group could continue to store personal data but not use it. This right is not absolute and in certain circumstances the Group can refuse a request.

vi. ***The right to portability***: to obtain and reuse their personal data for their own purposes across different services. The right only applies to information an individual has provided to the Group and where the lawful basis for processing is consent or performance of a contract. Paper records are excluded from this right.

vii. ***The right to object***: gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. The right effectively allows individuals to stop or prevent organisations from processing their personal data, though is not absolute and in certain circumstances the Group does not have to comply.

viii. ***Rights related to automated decision-making***: restricts organisations from making solely automated decisions, by enabling individuals to request human intervention or challenge a decision that has been made.

5.2 The legislation mandates that individual rights requests should be processed and responded to without undue delay but no later than one (1) calendar month from the date the request was received. To ensure compliance with the legislation the Group aims to process all requests within 28 days from the date it is received.

5.3 Individuals can make a rights request verbally or in writing, including via social media if directed at one of the Group's social media accounts. Individuals do not need to prescribe the legislation they are making the request under, and it is the responsibility of all staff to recognise when an individual rights request is being made and follow the correct procedure.

5.4 For further information and the detailed process and procedure for handling individual rights requests please see **Appendix 1** - DSAR - Group Process and **Appendix 2** - Data Subject Rights Request - Group Process.

## 6. Personal Data Breaches

6.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It can broadly be defined as a security incident that has affected the confidentiality, integrity, or availability of personal data.

6.2 There will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

6.3 All staff are responsible for ensuring the security of personal data and must comply with the Group's Data Breach Process, as outlined in **Appendix 3**.

## 7. Data Protection Impact Assessments (DPIAs)

7.1 The Group must carry out a DPIA for any type of processing of personal data, which is likely to result in a high risk to the rights and freedoms of individuals.

7.2 A DPIA is a process designed to help systematically analyse, identify, and minimise the DP risks of a project or change in processing and should be completed at the earliest opportunity in a project or change process. This will enable the facilitation of the legal requirement to imbed DP by 'design and default', through building in best practice and taking a privacy conscious approach.

7.3 All staff are responsible for seeking advice, at the earliest opportunity, from the DP team to establish whether a DPIA must be completed in relation to any new processing activity or change in the nature, process, or purpose of an existing process that uses personal data.

7.4 Detailed guidance on DPIAs, including when they are required as well as the correct process and procedure is set out in **Appendix 4** - DPIA - Group Process and must be followed by all staff.

## 8. Data Sharing and Disclosure

8.1 DP laws mandate that individuals' personal data must not be disclosed to any third party who does not have a legal right to access the information.

8.2 However, the legislation does not prevent the sharing of data if it is conducted in a fair, lawful and proportionate way. Data sharing has benefits and can on occasions it can be more harmful not to share data.

8.3 It is important that all staff follow the guidelines in this procedure, as failure to comply may put the Group and/or staff member in breach of the law.

8.4 Where data is incorrectly disclosed, the Data Subject has the right, under the DP laws, to seek compensation through the courts, as well as leave the Group open to enforcement action from the ICO including a fine of up to £17.5 million or four per cent of annual Group turnover.

8.5 Any data sharing by the Group must comply with the statutory code of practice for data sharing issued by the ICO - Data sharing: a code of practice.

8.6 A summary of the code is outlined below and must be completed prior to sharing any information with a third party:

(a) Consideration of whether a DPIA should be conducted (even if not legally obliged to do so),
(b) The identification of the purpose(s) and benefit(s) of the data sharing to all applicable parties, for example Sanctuary, society, individuals, third parties.
(c) Consideration of the governance arrangements, for example should the sharing be governed by a data sharing agreement, information sharing protocol or contract.
(d) Consideration of how the sharing complies with the DP principles to ensure it is lawful, fair and transparent.
(e) Consideration of how the Group can demonstrate it compliance with DP laws.
(f) Ensure appropriate security measures are in place to protect the confidentiality, integrity and availability of data.
(g) Consideration of the effect on individuals rights and how they can exercise these rights easily.

8.7 Emergency Situations

8.7.1 From time to time, there will be emergency situations that will not enable a detailed review of the lawfulness of sharing information as outlined in 8.5 and 8.6 above, prior to disclosing it.

8.7.2 In an emergency, staff should share data as is necessary and proportionate. Not every urgent situation will be an emergency. An emergency includes:

(a) preventing serious physical harm to a person;
(b) preventing loss of human life;
(c) protection of public health;
(d) safeguarding vulnerable adults or children; and/or
(e) responding to an emergency for example a request from the emergency services in a ‘blue light’ situation;

8.8 Requests by telephone

8.8.1 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 considered a standard ‘business as usual activity’ (BAU).

8.8.2 Staff must follow the relevant local guidelines for conducting DP checks before speaking to and disclosing personal data to service users over the phone.

8.8.3 It is best practice for staff to verify at least three personal account details with the customer to confirm who they are speaking to before sharing any personal or sensitive data. Details to check are:

- full name;
- full address and postcode;
- one other piece of information such as:
  - Date of birth

- Password
- Phone Number
- National Insurance Number.

8.9 Personal data requested on behalf of an individual by a third party.

8.9.1 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.

8.9.2 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 or the third party has lasting power of attorney (LPA) and the original request for data was in writing. Both consent, LPA and request letters must be held on file.

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

8.10 Data Processors

8.10.1 When personal data is processed by a third party, that is acting on behalf of the Group they will likely be a Data Processor. There are certain circumstances where a third party may be acting on the Group's instructions but be an independent Data Controller in their own right.

8.10.2 The Group has obligations to ensure that when engaging a Data Processor, that they adhere to the DP laws. Even when the Data Processor handles all personal data on behalf of the Group, any breaches of the DP laws are likely to impact the Group, as the Group would be the Data Controller and untimely responsible for the handling of the data, so it is imperative that the following steps are adhered to:

(a) it is a legal requirement that there is a written contract (or other legal act) in place between the Group and its Data Processors; and
(b) the agreement must contain clauses prescribed in the DP 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.

8.10.3 If staff have any uncertainty about whether they can share data, they should contact the DP team for guidance and support prior to any information being disclosed to a third party.

8.11 DSARs and Video Surveillance

8.11.1 Please see **Appendix 1** - DSAR - Group Process, for detailed guidance relating to requests for individuals' own personal data.

8.11.2 For the process of disclosure of video surveillance images please refer to the Video Surveillance Management Systems (VSMS) - Group Policy and procedure.

8.12 Gender Recognition Act 2004

8.12.1 Information relating to a person, regarding an application or granting of a gender recognition certificate must not be disclosed or shared unless in accordance with Section 22(4) of the Gender Recognition Act 2004.

## 9. Data Retention

9.1 DP law mandates that personal data must not be kept longer than is necessary for the purpose(s) for which it was obtained. It does not dictate how long personal data should be kept for. This means that personal data must be either anonymised, destroyed or erased from Group systems when it is no longer required.

9.2 All service areas are responsible for ensuring that the information processed within their area is aligned to an entry in the Group retention schedules and has a defined retention period or criteria for when the information should be disposed of.

9.3 All retention periods should be proportionate and justifiable in relation to the purposes for which the data was collected.

9.4 When setting a retention period, the following should be taken into consideration:

(a) Would the information be needed in future to defend any possible legal claims,
(b) Are there any legal or regulatory requirements which prescribe how long data should be retained,
(c) Are there any relevant industry standards or guidelines,
(d) Are there any circumstances or issues that could arise in the future that would require the retention of the data and if so, what time period are they likely to occur in.

9.5 All service areas are responsible for implementing appropriate processes and procedures for reviewing information held and anonymising, disposing, destroying, deleting information securely in line with the Group's retention schedules. This includes hard copy paper records or physical media, for example CDs, memory sticks or other mass storage devices.

9.6 All services areas should proactively manage data retention within their areas but as a minimum, data held should be reviewed annually against the Group's retention schedules, with information no longer required disposed of securely.

9.7 Data may be archived when access is no longer required day-to-day. However, archived data is still subject to the DP laws and the same requirements apply as outlined above.

9.8 When archiving hard copy information, to ensure that data is not lost appropriate documentation and logs must be kept recording what information is stored and its location. To prevent damage during storage, the storage space must be dry, and the data must be kept in the dark at normal room temperatures.

9.9 For archiving, storage must be either on the Group's premises or in spaces designated by the Group. For further details please refer to Archiving - Group Policy and Procedure.

9.10 Where Group systems enable automatic system level retention this should be configured to align to Group retention schedules and applied.

9.11 For clarification on the period that information should be retained for please refer to the Group's Retention Schedules, which should be read in conjunction with the Content and Records Management - Group Policy and Procedure.

## 10. Consent

10.1 Obtaining Consent

10.1.1 Consent is one of the lawful bases available to the Group under which it can process personal data.

10.1.2 Prior to collecting consent for a business process, the purpose of the processing should be clearly defined and provided at the point of collection through associated privacy information and statements.

10.1.3 For consent to be valid it must be freely given, specific, informed, and unambiguous. It must be obtained through a clear affirmative action, such as an individual providing their contact details, opting in via a checkbox or a similar mechanism.

10.1.4 All consent forms used by the Group should:

- Provide transparent information about the data being collected. This includes:
  i. **Purpose of data processing**: what the data will be used for.
  ii. **Types of data collected**: the categories of data that will be collected.
  iii. **Data recipients**: whether the data will be shared with or processed by any third parties on Sanctuary's behalf.
  iv. **Retention**: how long their data will be stored for and how long the consent will remain valid for.
  v. **Rights of individuals**: inform individuals about their rights regarding their personal data and how to exercise a rights request.
  vi. **Consent withdrawal**: explain how individuals can withdraw their consent at any time.

10.1.5 Provide granular consent options to give individuals choice and control over their personal data and use.

10.1.6 Obtain consent through clear affirmative action such as ticking a box or signing a form.

10.1.7 The Group should provide individuals with options to update their consent preferences easily such as through an online portal or e-mail communication.

10.1.8 Where collecting 'explicit' consent for the processing of 'special category' data, this must:

i. be separate from other consents being collected; and
ii. include a dedicated statement explaining the purpose the data will be used for and that Data Subject consents to this processing.

10.1.9 Where consent has been obtained, appropriate records must be kept and maintained. This should include:

(a) the specifics of what has been consented to;
(b) the date consent was obtained;
(c) a brief description of how it was obtained;
(d) the length of time it remains valid for and when it should be refreshed; and
(e) details of the specific privacy information provided to individuals at the time of obtaining consent.

10.1.10 All communications related to the collection of consent should be transparent and in plain English. Individuals should be informed of how their data will be processed, shared, and protected, as well as their DP rights regarding data processing activities. This transparency activity is delivered via a Group privacy statement that also provides individuals with the contact details to exercise a Data Subject rights request.

10.2 Consent Refresh

10.2.1 Consent refresh refers to the practice of reviewing and renewing consent obtained from individuals for the processing of their personal data to ensure that it remains valid, relevant, and compliant with the Group's obligations as a Data Controller.

10.2.2 ICO guidance outlines consents should be considered for refreshing every two years. However, this is not mandatory and may not be appropriate in all circumstances considering the specifics and context of the processing. When determining whether consent should be refreshed, the following should be taken into consideration and the rationale for the decision taken documented:

i. people's expectations - what would a reasonable person expect the frequency to be;
ii. is the Group in regular contact with individuals; and
iii. how disruptive to individuals would it be to make repeated consent requests.

10.2.3 The criteria for triggering a mandatory consent refresh exercise are:

i. Expiration of consent validity period.
ii. Material changes in data processing activities. For example, if the Group intends:
(a) to use the personal data for a new or additional purpose;
(b) share the data with a new or additional third party;
(c) process additional categories of personal data; and
(d) process/retain the data for longer than originally outlined.

10.2.4 When refreshing consent, the following activities should be undertaken to ensure the consent remains valid:

i. proactively contact individuals to refresh their consent;
ii. clearly communicate the reasons for requesting consent refresh and provide updated information on data processing practises;
iii. offer individuals the option to easily update or revoke their consent preferences at any time; and
iv. document the process of refreshing concerned including the date of the request and the individual's response.

10.3 Withdrawal of Consent

10.3.1 Individuals have the absolute right to withdraw their consent at any time. The Group must provide simple and easily accessible methods for individuals to withdraw consent, such as an unsubscribe link in email communications or the provision of an email address to submit their request to.

10.3.2 Once consent is withdrawn, the individual's request must be actioned promptly without undue delay so that they receive no further marketing communications.

10.3.3 Where data is shared with third parties, the request of the Data Subject should be conveyed to all third parties to action appropriately and records kept to document this.

10.3.4 All service areas are responsible for implementing appropriate processes and procedures for reviewing consents held and ensuring they remain valid, relevant and compliant.

10.4 For further information on consent and requirements related to marketing activities, please refer to **Appendix 5** - Marketing - Group Process.

## 11. International Data Transfers

11.1 When data is transferred outside the UK people risk losing the protection of the DP legislation. The UK GDPR contains rules on the transfer of personal data to receivers located outside the UK, which are separate controllers or processors and legally distinct from the Group. These rules apply to all transfers, no matter the size of transfer or how often the Group carries them out.

11.2 The Group may make a restricted transfer if the receiver is located in a third country or territory, or is an international organisation, covered by UK 'adequacy regulations' in accordance with Article 45 of the UK GDPR.

11.3 A list of the countries deemed adequate by the Secretary of State for Digital, Culture, Media and Sport is available from the Government website.

11.4 When the Group is proposing to make a restricted transfer to a country that does not have an adequacy decision, a Transfer Risk Assessment (TRA) must be conducted using the latest published ICO TRA tool and guidance.

11.5 If the assessment concludes that a restricted transfer can proceed the Group must implement appropriate safeguards in the form of Standard Contractual Clauses issued by Secretary of State in accordance with Article 46 of the UK GDPR:

- International Data Transfer Agreement (IDTA); or
- the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers (UK Addendum).

11.6 In limited circumstances the Group can apply an appropriate exemption in accordance with Article 49 of the UK GDPR, the basis of which must be documented in the associated TRA.

11.7 Where a Data Processor acting on the Group's behalf proposes to make a restricted transfer, the Group must undertake appropriate due diligence to ensure the transfer can be made lawfully.

11.8 To achieve this the Group must be provided with a copy of the associated TRA and appropriate safeguards to review to ensure they are robust and compliant.

11.9 All TRAs should be reviewed annually as a minimum or when material changes to the processing are proposed or the circumstances in the destination country change.

## 12. Data Protection at Sanctuary

12.1 DP team

12.1.1 The DP team is responsible for providing assurance to Executive about the Group's compliance with data protection regulations.

12.1.2 The DP team supports the Group by providing technical advice and guidance on data protection matters and the steps required to achieve compliance.

12.1.3 The team monitor compliance ensuring associated documents and registers are regularly reviewed and updated by the relevant business area so that they remain accurate to comply with the legislation.

12.1.4 The team have responsibility for oversight of DP risk management across the Group.

12.2 Designated Officer Network

12.2.1 The Group is a large and complex organisation. To help achieve and support compliance the Group has implemented a network of DOs.

12.2.2 DOs are DP champions within their relevant business areas responsible for supporting compliance. The role of a DO includes promoting key DP principles, raising awareness of individuals' rights and the processes that support them as well as supporting staff with basic DP queries and sign posting to the DP team when detailed technical guidance is required.

12.2.3 The DO Network operates in a 'Hub and Spoke' model with the DP team at the centre providing advice, guidance and setting the compliance work programme and requirements. These requirements are then delivered by the DO network and reported to the Data Governance Forum.

12.2.4 All business and services areas must have appropriate DO coverage and resources in place to facilitate compliance and the associated activities issued by the DP team.

12.2.5 The DP team support the DO Network by providing:

(a) quarterly DO network meetings;
(b) monthly informal drop-in session;
(c) FAQs and awareness materials;
(d) direction on compliance requirements and timescales for completion;
(e) a point for escalation for operational DP matters; and
(f) updates to DP legislation and what that means for each business area.

12.2.6 All DOs must complete the mandatory DO Training within 30 days of appointment.

12.2.7 For further guidance on how DOs support DP compliance across the Group, please refer to **Appendix 6** - DO Role and Responsibilities.

12.3 Data Owners

12.3.1 A Data Owner is responsible for the data within their respective business area and form part of the Data Governance Forum.

12.3.2 Data Owners are responsible for ensuring that the data within their domain is governed throughout the organisation and in compliance with DP.

12.3.3 Data Owners are responsible for appointing DOs within their domain and ensuring required compliance activities are undertaken and within required timeframes.

12.3.4 All business areas must have appropriate Data Owner coverage to facilitate compliance and the associated activities issued by the DP team.

12.3.5 For further guidance on how Data Owners support DP compliance across the group, please refer to **Appendix 7** - Data Owner Role and Responsibilities.

## 13. Compliance Requirements and Activities

13.1 The DP team is responsible for setting the Group's DP Work Programme and associated compliance activities, which are delivered in partnership with the DO Network and Data Owners.

13.2 Records of Processing Activities (RoPA)

13.2.1 A RoPA is an internal document that records all the processing activities undertaken by an organisation which involve the use of personal data. It is a mandatory requirement under DP legislation for an organisation of Sanctuary's size and is the corner stone of demonstrating compliance with the accountability principle.

13.2.2 All business areas must have a RoPA in place that accurately records their processing activities involving personal date, including details of the:

(a) purpose of processing;
(b) categories of individuals;
(c) categories of personal data;
(d) source of the personal data;
(e) location of where the personal data is saved or stored;
(f) details of Data Processors and their purpose;
(g) categories of recipients of who personal data is shared with;
(h) names of third countries or international organisations that personal data is transferred to (if applicable);
(i) retention period or criteria for disposal and associated Group retention schedule reference;
(j) lawful basis for processing;
(k) existence of automated decision making or profiling;
(l) name and contact details of joint controllers (if applicable);
(m) description of technical and organisational security measures;
(n) safeguards for restricted transfers (if applicable);
(o) article 9 condition of processing for special category data (if applicable),
(p) DPA 18 Schedule 1 Condition for processing special category data (if applicable);
(q) Legitimate interest reference number (if applicable);
(r) DPIA reference number (if applicable); and
(s) Appropriate Policy Document reference number (if applicable).

13.2.3 Best practice outlines that a RoPA should be treated as a living document, which means it should be updated each time there is a change to our data processing activities, such as sharing information with a new third party, or when we start collecting new categories of personal data for a new purpose or service.

13.2.4 However, it is recognised that this will not always be practical or possible but as a minimum each business area must review and update their RoPA to ensure it remains fit for purpose and accurate, annually.

13.2.5 All RoPAs must be signed off by the relevant Data Owner as a true and accurate record.

13.2.6 The DP team oversee and support this process by outlining required timescales for completion as well as providing technical support, guidance.

13.3 Privacy statements

13.3.1 As outlined in section 4.3 the Group must make certain privacy information available to Data Subjects relating to the processing of their personal data in the form of a privacy statement.

13.3.2 Privacy statements must be kept up to date and amended to reflect any changes in processing as and when they arise. DOs are responsible for notifying the DP team of any changes, who will provide support to ensure statement(s) are compliant.

13.3.3 When a privacy statement is updated, a description of the changes and date made should be recorded in the ‘what’s new section’ to ensure transparency.

13.3.4 Each business area within the Group is responsible for providing individuals with privacy information at the point information is collected.

13.3.5 At a minimum all Group privacy statements must be reviewed annually to ensure they are accurate and remain fit for purpose.

13.3.6 The DP team oversee and support this process by outlining required timescales for completion as well as providing technical support, guidance and maintaining the Group’s central register.

13.4 Data Protection Impact Assessments (DPIAs)

13.4.1 As outlined in section 7, the Group must conduct a DPIA for any high-risk processing that could affect the rights and freedoms of individuals.

13.4.2 A DPIA should be treated as a ‘living document’ and updated when the associated processing changes to consider any new risks emerging or if any have been mitigated as a result. Best practice dictates that this should be done in real time prior to any changes being implemented.

13.4.3 However, to ensure DPIAs remain accurate, an annual review of any live DPIAs should be conducted as a minimum. These reviews should be led by the owner of the DPIA; however, if that individual has changed role or left the business the DP team will work in partnership with the relevant Data Owner and DO to identify an appropriate owner.

13.4.4 The DP team hold the central register of DPIAs and will lead the review process and issue instructions and guidance as appropriate.

13.5 Legitimate Interests Assessments (LIAs)

13.5.1 Whenever Legitimate interests is relied upon as the lawful basis for processing personal data a legitimate interest assessment must be completed that considers the specific context and circumstances of the processing:

(a) *Purpose test*: is the Group pursuing a legitimate interest?
(b) *Necessity test*: is the processing necessary for that purpose?
(c) *Balancing test*: do the individual's interests override the Group's legitimate interest?

13.5.2 The only exception to this is where a DPIA has been completed for the associated processing as the above requirements would be considered and documented as part of the DPIA process.

13.5.3 The legitimate interests can be Sanctuary's own interests or the interests of third parties. They can include commercial interests, individual interests, or broader societal benefits.

13.5.4 If the Group chooses to rely on legitimate interests as it's lawful basis, it must consider and protect people's rights and interests.

13.5.5 As with other compliance documents LIAs should be treated as a 'living document' and updated when the associated processing changes.

13.5.6 However, to ensure LIAs remain accurate, an annual review of any live LIAs should be conducted as a minimum. These reviews should be led by the owner of the LIA; however, if that individual has changed role or left the business the DP team will work in partnership with the relevant Data Owner and DO to identify an appropriate owner.

13.5.7 The DP team hold the central register for LIAs and will lead the review process and issue instructions and guidance as appropriate.

13.6 Data Retention

13.6.1 As outlined in section 9, all service areas are responsible for implementing appropriate processes and procedures for reviewing and disposing of information securely in line with the Group's retention schedules.

13.6.2 As part of the Group's DP compliance activities the DP team will perform audits across the Group to provide assurance to Executive that the Group is applying its retention schedules appropriately.

13.6.3 Where non-compliance is identified the DP team will work with the relevant Data Owner(s) and DO(s) to implement appropriate mitigation actions.

13.7 Appropriate Policy Document (APD)

13.7.1 When the Group processes special category and or criminal offence data, in certain circumstances the DPA 18 requires an APD to be in place. An APD is a short document that sets out the Group's compliance measures and retention policies for special category and criminal offence data.

13.7.2 An APD should include details of:

(a) the Schedule 1 condition (or conditions) we are relying on;
(b) the procedures for complying with each of the DP principles;
(c) the retention and deletion policies; and
(d) the retention period or criteria for disposal for the specific data.

13.7.3 Whenever any of the following conditions as outlined in Schedule 1 of the DPA 18 are relied upon to process special category or criminal offence data an APD must be in place:

1. Employment, social security and social protection,
6. Statutory and government purposes
7. Administration of justice and parliamentary purposes,
10. Preventing or detecting unlawful acts.
11. Protecting the public
12. Regulatory requirements
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
17. Counselling
18. Safeguarding of children and individuals at risk
20. Insurance
24. Disclosure to elected representatives
26. Publication of legal judgments

13.7.4 All APDs must be retained for a minimum of six months after the date the associated processing stops, though they can be retained for longer depending on the nature of the processing and business need.

13.7.5 APD should be updated in alignment with changes to the processing, however, to ensure APDs remain accurate, an annual review of any live APD should be conducted as a minimum.

13.7.6 The DP team hold the central register for APDs and will lead the review process and issue instructions and guidance as appropriate.

13.8 Consent

13.8.1 The DP team will perform audits across the Group to provide assurance to Executive that where the Group is relying on consent as the lawful basis for processing it is compliant.

13.8.2 Where non-compliance is identified the DP team will work with the relevant Data Owner(s) and DO(s) to implement appropriate mitigation actions.

## 13.9 Training

13.9.1 The DP team is responsible for annually reviewing the Group's mandatory DP and DO training to ensure it remains fit for purpose.