Title: **Data Protection - Group Policy**

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

Authors: **Data Protection team**

Authorised by: **Executive Committee**

1. Policy statement

1.1 Sanctuary Group (the Group) collects and uses personal information about the people with whom it works in order to operate efficiently and effectively in the provision of high quality services to its customers, whilst meeting its obligations to comply with regulatory and legal requirements, specifically Data Protection (DP) legislation including the DP Act 2018, United Kingdom General DP Regulation and The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (the DP laws). The Group's customers include current and past service users, current, past and prospective employees, clients and customers, suppliers and any other persons acting on behalf of the Group.

1.2 The purpose of this policy is to support all staff in complying with the obligations of the DP laws through following the seven key principles of the UK General DP Regulations (UK GDPR), and to ensure that the Group maintains good practices in relation to DP.

1.3 The Group does all that it can to ensure staff who record personal data do so on a factual and impartial basis, and that terminology used could not cause offence in future disclosures.

1.4 Such personal information, however, it is collected, recorded, and used, must be handled and dealt with in a proper and appropriate manner to ensure compliance with the DP laws, thereby safeguarding the data the Group holds on individuals. Information may be held on paper, in computer records or recorded by any other means, and there are measures in place to ensure that personal data is kept secure at all times against unauthorised use or unlawful loss or disclosure.

1.5 The Group is fully committed to operating within the requirements of the DP laws and has developed its policies and procedures to ensure that all personal data is handled in compliance with the DP laws and to ensure that all service users, staff and contractors are fully aware of and comply with their duties under the DP laws. In addition, everyone managing and handling personal information understands that they are contractually responsible for following good DP practice.

1.6 It is vital that all staff involved in the managing and handling of personal information are appropriately trained and supervised. It is important that staff recognise that they as individuals are also responsible under the DP laws and can be personally liable for any breaches. Such breaches could result in disciplinary action, where appropriate.

1.7 Any queries about the handling of personal information and requests from individuals for their personal data must be dealt with promptly and courteously by Group staff. Data sharing, and data disclosure must generally be carried out under a written agreement that sets out the scope and limits of the sharing/ disclosure compliant with this policy and its procedure. Data sharing without a written agreement in place must only be done where there is a clear lawful mechanism to do so under the DP laws (for example, a disclosure of

information to the police for the purposes of a criminal investigation). If there is uncertainty about whether information can be lawfully shared or disclosed, the DP team must be consulted before any data is shared.

1.8 This policy should be read in conjunction with the following:

- DP - Group Procedure
- 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

1.9 The following appendices to the DP - Group Procedure form part of this policy:

- **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

2. Legislative/Regulatory Context

2.1 This policy 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. Roles and responsibilities

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

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

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

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

3.5 Designated Officers 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. References and sources

- Data Protection Act 2018
- United Kingdom General Data Protection Regulation (UK GDPR)
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulation 2000 (LBP Regulations)
- Telecommunications (Data Protection and Privacy) Regulations 1999
- Gender Recognition Act 2004
- Human Rights Act 1998
- 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) - Policy and Procedure Group
- Inclusion for All - Equality, Diversity and Inclusion Strategy 2024 - 2026

5. Impact on diversity

5.1 This policy applies to all functions across the Group and is therefore relevant to all staff.

5.2 The Group demonstrates its commitment to diversity and promoting equality by ensuring that this policy is applied in a manner that is fair to all sections of the community, with due regard to the protected characteristics identified under the Equality Act 2010 and in accordance with the 'Sanctuary Inclusion for All Strategy 2024-2026'.

6. External consultation

6.1 There is no requirement for external consultation on this policy as it relates to the internal procedures for complying with DP, the requirements for which are driven by legislation.

7. Monitoring and compliance

7.1 This policy is relevant Groupwide, and ongoing compliance will be ensured by a close working relationship between the DP team, Data Owners, and Designated Officers across the Group's operations and functions. Data Owners and Designated Officers will be updated on changes driven by legislation or communications from the Information Commissioner's Office, regularly via meetings of the Data Governance Forum and Designated Officer Forum.

7.2 Period of review

7.2.1 Until a new policy is formally adopted this document will remain in force and operational.

7.2.2 This policy will be reviewed in accordance with the policy review programme agreed by Executive Committee.

7.2.3 If there are significant changes to legislation or regulation or there are found to be deficiencies or failures in this policy, as a result of complaints or findings from any independent organisations, the Executive Director - Corporate Services or DP team will initiate an immediate review.

7.2.4 Where appropriate, key stakeholders and interested parties will be consulted as part of any review of this policy.

8. Approval

8.1 This policy is approved by Sanctuary Group's Executive Committee.

9. Operational arrangements

9.1 This policy is accompanied by the DP - Group Procedure and supporting documentation and appendices, which are available on Solis.