Title: **Content and Records Management - Group Policy**

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

Authors: **Data Protection**
Technology

Authorised by: **Executive Committee**

1. Policy statement

1.1 Sanctuary Group's (the Group's) mission is to build affordable homes and sustainable communities where people choose to live. The Group's strategic priorities include engaging with its customers and stakeholders, and to invest in its homes and communities**.**

1.2 This policy helps us meet our legal and regulatory responsibilities when it comes to managing information and records. It sets out how we manage records from the moment they are created or received, stored, and eventually deleted or archived. This applies to all records, whether they are digital or paper-based, and whether they come from inside or outside the organisation.

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

- Data Protection - Group Policy and Procedure
- Archiving - Group Policy and Procedure
- Video Surveillance Management Systems (VSMS) - Group Policy and Procedure
- Disciplinary - Group Procedure
- Flexible Working - Group Procedure
- Acceptable Usage - Group Policy and Procedure
- Third-Party Access - Group Policy and Procedure
- Information Security - Group Policy
- Information Security Management System Manual.

1.4 The following appendices to the Content and Records Management - Group Procedure form part of this policy:

- Appendix 1 - Retention Schedule
- Appendix 2 - Content and Record Retention Flowchart
- Appendix 3 - Naming Conventions

1.5 Definitions

1.5.1 We use information and records to run our services and meet our responsibilities. Some key terms are:

- **Content**: Information that is stored but can be subject to change.
- **Record**: Final version (can no longer be changed) of any information we create or receive that we keep as evidence or for business reasons. This could be on paper or in digital form. Version control must be used when updating a record and superseded versions must be archived.
- **Document**: A written, printed, or digital file that provides information or acts as an official record.
- **Retention Schedule**: A guide that tells us how long we need to keep different types of records before we can safely archive, then destroy or delete them.

1.5.2 Our records and documents help us run our services smoothly, meet legal requirements, and show that we are acting responsibly. They are valuable assets that provide useful information for day-to-day work, decision-making, and understanding what we have done in the past.

1.5.3 By following this policy, we can:

- Keep our records and documents organised and well-managed.
- Make sure we have reliable information to support decisions.
- Deliver services more efficiently.
- Protect the rights and interests of our customers, staff, and the organisation.
- Make sure the right people can access the right information when they need it.

1.6 Record Management Principles

1.6.1 The Group follows a set of principles to make sure information and records are managed properly. We will:

- Use information and records only for the purpose they were collected.
- Keep only the information we need and are allowed to store.
- Manage records in line with laws, regulations, and recognised best practices.
- Safely delete or archive records that are no longer needed, based on how sensitive they are and how long we're required to keep them.

1.7 Useful resources

- For general guidance on how long to keep records, see Section 9 of the Data Protection - Group Procedure (pages 23-24).
- For help deciding how long to keep specific records, check the Retention Schedule on Pulse.
- Designated Officers as well as the Data Protection Team are available to support teams with retention planning.
- If records are kept based on someone's consent, this must follow the rules in Section 10 of the Data Protection - Group Procedure (pages 24-26). The Data Protection Team can also help with questions about managing consent.

1.8 Classifying Information

1.8.1 All records and content should be given a sensitivity classification to show how important or private they are. This helps us protect information properly and reduce the risks of something being shared to or accessed by the wrong people.

1.8.2 You can apply sensitivity labels in standard Microsoft applications by using the "Sensitivity" option on the Menu Ribbon, from the Title Bar or when saving a document.

1.8.3 Using these labels helps us apply Data Loss Prevention (DLP) tools and processes across the Group, making sure sensitive information is protected appropriately.

Table 1: Sensitivity Classification summary and examples

Category	Access Level	Examples
Public	This information can be used by everyone inside or outside of Sanctuary.	Public announcements, services offered, FAQs, Social Media Posts, Public Policy Documents, Public Reports, Supplier Guidelines, Public Event Information, Published Marketing Materials
Internal Only	Documents which do not contain highly sensitive information and should not be shared externally to Sanctuary in normal circumstances. There may be occasions where information is needed to be shared with trusted external parties for known business purposes but must be checked before sharing externally.	Internal event information, educational content for staff development, non-confidential minutes from internal meetings, non-sensitive internal communication, external party meeting actions and minutes (non-sensitive), system or product specifications or requirements, testing results, sales, and marketing information (not public).
Confidential	Data that is sensitive but should not be readily shared externally except with specific external trusted partners for known business purposes and with controls in place. User discretion is advised.	Tenant personal information, Monthly performance reports, resident and tenant feedback, Supplier Agreements, Housing, and care agreements shared with funding bodies, Commercial contracts, and leases.
Highly Confidential	Highly confidential data that must be strictly controlled and not shared outside of Sanctuary except with specific external trusted partners under strict terms, such as contractual agreements or non-disclosure agreements (NDAs), care plans shared with the NHS.	HR Data, Legal Documents, Special Category of Customer Data, Care plans, Financial reports shared with auditing firms, Legal documents shared with contracted external legal providers and negotiations

1.9 Retention and Disposal

1.9.1 We keep records for a set amount of time, based on the Group's retention schedule. The clock starts ticking once the record has served its purpose and is no longer actively being used (post processing). Examples:

- A customer fills out a web form asking for service details. Once we have responded and closed the request, the record enters its retention period.
- A performance report created for a year-end meeting enters its retention period after the meeting is held.
- Documents and records relating to a project enter their retention period following the formal closure of the project.
- A policy document is updated, and a new version is published. Once the new version is published the old policy enters its retention period.

1.9.2 All records that include personal information must follow the retention timelines listed in the Group's Retention Schedule; this includes any physical records. For more details, see the Data Protection - Group Policy and related procedures.

1.9.3 Additionally if you're handling physical records (like paper files), follow the guidance in the Archiving - Group Policy.

1.9.4 Even if a record does not contain personal data, it still needs a clear retention period to help us avoid keeping unnecessary information and reduce our physical and digital storage costs as well as the associated environmental impact.

1.9.5 If a specific time limit cannot be set, the criteria that will be applied to determine when it should be disposed of, including the supporting reasons must be documented to demonstrate how that decision was made.

1.10 Legal Hold

1.10.1 Sometimes, records that are in their retention period may need to be kept longer due to legal or regulatory reasons. For example, if they are needed for a legal case or investigation.

1.10.2 In these cases:

- Digital records should be placed under a "Legal Hold" to stop them from being deleted.
- Paper records should be retrieved and stored securely until the issue is resolved.

1.10.3 Once the legal need is over, the record should be aligned back to its original retention period.

1.10.4 For more details, see **Section 14** of the Archiving - Group Procedure (page 8).

2. Policy Scope

2.1 This policy covers **all records** held by Sanctuary Group, no matter the format - paper, digital, or other media. Records must be classified based on how sensitive they are and what the impact would be if they were lost or shared inappropriately.

2.2 It applies to:

- All systems, equipment, and facilities that store or process Group information.
- Anyone accessing Group data, whether on-site or working remotely (including from home).

2.3 For more guidance, see the Acceptable Usage - Group Policy.

3. Roles and responsibilities

3.1 Managing information and records is a shared responsibility across the Group.

- Executive Committee: Oversees records and information management at a strategic level.
- Directors (or equivalent) are responsible for ensuring adoption of and adherence to this policy.
- Managers are responsible for applying this policy in day-to-day operations and ensuring all their staff comply.
- All Staff (including temps, contractors, and consultants) must read and follow this policy when handling records and information.
- Data Custodians are accountable for ensuring records that fall within data protection laws (UK GDPR, DPA 2018, Privacy and Electronic Communications Regulations 2003) are documented within the Group's retention schedule and managed accordingly, including the disposal of information, data, documents, and records.
- Designated Officers support operational regulatory compliance with data protection legislation.
- The Data Protection Team is responsible for providing advice and guidance to support appropriate retention of information, data, documents, and records.
- The Technology department facilitate the automation of data retention held in Group systems in accordance with the Group's retention schedule and business requirements.
- Technology Security are responsible for securing, protecting, and monitoring data usage.

4. References and sources

- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulation (UK GDPR)
- Health Records Act 1990
- National Housing Federation - Document retention and disposal for housing associations

5. Impact on diversity

5.1 This policy applies to all employees and contractors as outlined above.

5.2 Sanctuary 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. Customer consultation

6.1 This policy and the associated procedure is for the management of Sanctuary's information and records, driven by data protection and data security requirements - therefore, no customer consultation has been done.

7. Monitoring and compliance

7.1 This policy and its associated procedure will be reviewed by the Data Protection Team with support from the Technology department to ensure continued relevance and effectiveness.

7.2 The Group's Retention Schedule will be reviewed annually to maintain compliance with regulatory and operational requirements.

7.3 Period of review

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

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

7.3.3 If there are significant changes to legislation or regulation or there are found to be deficiencies or failures in this policy, because of complaints or findings from any independent organisations, the Executive Director - Corporate Services and/or the Director for Governance and Legal Services will initiate an immediate review.

7.3.4 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's Executive Committee.

9. Operational arrangements

9.1 This policy is accompanied by the Content and Records Management - Group Procedure and supporting documentation and appendices, which are available on Pulse.