POLICY DOCUMENT
Data Retention Policy

POLICY TITLE:	**Data Retention Policy**
LEAD OFFICER:	**ICT Service Manager**
DATE APPROVED:	**TBC**
APPROVED BY:	**TBC**
IMPLEMENTATION DATE:	**August 2024**
DATE FOR NEXT REVIEW:	**August 2028**
ADDITIONAL GUIDANCE:	**Data Protection Policy** **Freedom Of Information Policy**
ASSOCIATED CUSTOMER PUBLICATIONS:	**None**
TEAMS AFFECTED:	**All SLHD Teams**
THIS POLICY REPLACES	**Data Retention Policy v5**

DOCUMENT CONTROL

For guidance on completing this section please refer to the document version control guidance notes

Revision History

Date of this revision:	August 2024
Date of next review:	August 2028
Responsible Officer:	ICT Service Manager

Version Number	Version Date	Author/Group commenting	Summary of Changes
1.0	May 2006	Central Support Team Leader	Initial release
2.0	Feb 2010	Central Support Team Leader	Revised and extended policy, to include contracts and agreements
3.0	February 2014	Head of ICT	Revision to timescales for retaining accounting docs and also certain FTA documents. Extended range of documents for a number of service areas, particularly Health & Safety, and inclusion of Private Landlord documents. Also clarification on storage of documents held on core SLH IT systems
4.0	Aug 2017	ICT Service Manager	Revisions following Annual Review. Extended to cater for introduction of Strategic Housing to SLHD.
4.1	Aug 2020	ICT Service Manager	Policy Title renamed from Document to Data Policy. 1.1 amended DP Act from 1998 to 2018 5.1 amended to include a link to the information asset register Appendix 1 removed.
5.0	Aug 2020	EMT	Approved
6.0	Aug 2024	ICT Service Manager	The policy has been re-written to clarify that this policy covers all documents and data. Section 5 – Clarified what an IAR is and it’s purpose within the organisation. Updated the link to the IAR document. Section 7.1 – amended to say SMT will review the IAR annually.

Policy Creation and Review Checklist

Action	Responsible Officer	Date Completed
Best practice researched (Housemark, HQN, Audit Commission, general websites)	ICT Service Manager	May 2024
Review current practices from similar organisations	ICT Service Manager	May 2024
Review customer satisfaction data from the area the policy relates to	N/A	
Review Customer complaints from the area the policy relates to	N/A	
Undertake customer consultation if applicable	N/A	
Staff consultation if applicable	ICT Service Manager	August 2024
Trade Union consultation if applicable	N/A	
Stakeholder consultation if applicable	N/A	
Equality impact assessment carried out online	ICT Service Manager	August 2024

NB. The above table must be completed on all occasions. The policy will not be accepted or approved by EMT without this information completed.

POLICY DOCUMENT
Data Retention

1. Introduction

1.1 We need to keep records, in an organised, secure, digital filing system that is easy to manage and access, of our business activities, decisions and history, according to the policies and procedures we have adopted. This policy will help us manage our documents and data appropriately, and provide a consistent way to store them, electronically by default as part of our Digital First approach and paper only where necessary. It will stop us from destroying records too early and will make sure we keep relevant information for as long as it is needed to follow legal, financial and statutory requirements. In particular, it will support the Freedom of Information Act 2000 that allows people to access information we hold that is not exempt, and also the UK GDPR and Data Protection Act 2018 that requires us not to keep personal data longer than necessary.

2. Purpose

2.1 The purpose of a Data Retention Policy is to provide a systematic approach to managing data, ensuring compliance with legal and regulatory requirements, supporting disaster recovery, and enhancing efficiency by retaining data only as long as necessary.

3. Scope

3.1 The policy covers all the documents and data that are received by the organisation and all the documents and data that are generated and sent out by the organisation, across all service areas, and are defined within the Information Asset Register.

4. Responsibilities

4.1 The overall responsibility for the data retention policy sits with the ICT Service Manager. However operationally it is the responsibility of all service managers and information asset owners to ensure that the policy is adhered to by all employees.

It is the data owners responsibility to ensure that any documents and data is only kept in line with what the policy states for that specific type. It is also their responsibility for the secure destruction of any information after this date.

5. Policy

5.1 An Information Asset Register (IAR) is used within St. Leger Homes to record and manage information assets.

For each asset listed in the IAR, further information is recorded, such as: the type of document, how and where it is stored, the retention period and ultimately who is the responsible owner of the asset.

5.2 The IAR outlines the primary use of the asset and helps to identify any areas of duplication, or high risk. A key marker on the IAR is to identify any Sensitive Personal Data, being able to identify these assets means the relevant security protocols can be implemented.

5.3 The Information Asset Owner (IAO) is the individual that is responsible for ensuring the asset is maintained correctly. The IAO should be aware of any risks associated with the asset and that mitigation is in place.

5.4 The detailed Information Asset Register covering the range of documents can be accessed by clicking on the link below.

Information Asset Register

6. Consultation

6.1 There was a need for extensive consultation with the Senior Management Team (SMT) when the Information Asset Register was first created, reflecting the range of documents in the organisation and to ensure it takes account of the statutory and recommended retention periods.

7. Monitoring and Review

7.1 The policy will be formally reviewed every 4 years. However almost certainly there will be changes to data and document types within that period, specifically the addition of new data sets and documents. In addition, there may well be legislative changes that may affect the period we need to retain certain documents.

Therefore the Information Asset Register will be reviewed annually by SMT and the register would be updated to reflect the revised retention periods and/or data sets.

8. Partnership issues

8.1 We will collaborate with City of Doncaster Council (CDC) to implement this policy, especially the data retention features of the corporate EDRMS (electronic document records management system).