



Building a better future - together



Data Retention & Disposal Policy

Document ID/Version:	Version 1 - new integrated Policy for SettleParadigm			
Executive Lead (Owner):	Group General Counsel			
Policy Author:	Data Protection Manager			
Strategic alignment:	The Policy fulfils a Legal Requirement.			
Review frequency:	Every 3 years	☒	Other (state period)	
Previous review date:	September 2022 (Paradigm) March 2018 (Settle)			
Date policy approved:	July 2026			
Policy approved by:	Executive Board			
Next policy review date:	July 2029			
IMPACT ASSESSMENTS				
Equality Impact Assessment				
Completed?	No	☐	Yes	☒
	If not required, state reason:			
Resident Impact Assessment				
1) Is this one of the agreed policies requiring resident consultation? Please refer to:	Yes	☐	No	☒
2) If yes, please confirm resident consultation has taken place	☐	Briefly detail changes arising from resident feedback:		
APPROVAL - To show transparency and accountability, specify whether policies have been approved by the Board/Executive/Committee. Clear approval lines strengthen governance, ensuring assurance and accountability.				
Approval journey:	Executive Team	Committee		Board
		Yes	Committee name(s)	
	☒	☐		☐
Which Regulatory Standard does this Policy support?	Economic			
	Governance & Viability	Rent		Value for Money
	☒	☐		☐
	Consumer			
	Neighbourhood & Community	Safety & Quality	Tenancy	Transparency, Influence & Accountability
	☐	☐	☐	☐
Associated legislation	The Policy is driven by Data Protection Law as listed below and			

	the retention schedule is driven by a variety of regulations, laws and guidance as set out and listed in the schedule itself Relevant Data Protection Law • Data Protection Act 2018 • UK General Data Protection Regulation (UK GDPR) • The Data Use & Access Act 2025		
Associated procedures	Annual Weeding Exercises		
Where is this policy to be published?	Website	Intranet	Both
	☐	☐	☒

Data Retention & Disposal Policy

1. Policy Statement

This policy sets out our approach to the retention and disposal of information across all business areas, covering electronic and hard copy data.

It is a requirement under UK Data Protection law that personal data is limited to what is necessary and kept for no longer than is necessary for the purposes for which it is processed. Other laws will apply to different record types (such as company and finance records) some of which must be retained indefinitely.

There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

2. Objectives, desired outcomes and strategic alignment

The objective of this policy, and associated record retention schedule, is to provide clear guidance on our approach to managing the retention and secure disposal of our information in line with business requirements and legal obligations. Our record Retention Schedule has been aligned with National Housing Federation (NHF) guidance and relevant retention periods are also noted in our Records of Processing Activities (ROPA).

3. Scope

This Policy applies to all business units and functions of our business. It is applicable to all employees, whether full-time or temporary, consultants, Board / Committee / Panel Members, volunteers, and all users of SettleParadigm infrastructure, information systems, networks, and applications and those supplied under contract to us. It covers data that is held and processed by third parties on our behalf. It covers the retention and disposal of all electronic and hard copy business information including, but not limited to:

- personal data (data from which living individuals can be identified) including audio and video recordings and CCTV recordings,
- company records such as company incorporation documents,
- operational records such as procedural documentation or similar,

- other records of appreciable value to the organisation such as accounting records, finance records, regulatory or similar.

4. Policy Principles

We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason. Information will be retained only for as long as there is a valid reason for doing so, such as a legal requirement or best practice standard. We also handle, store and dispose of data responsibly and securely;

Information will not be retained where it is known to be out of date or where there is reason to believe it is incomplete. In both these cases, information must either be updated, completed, securely disposed of, or deleted.

For personal data (data from which living individuals can be identified) UK Data Protection law applies. It dictates that records are limited to what is necessary and kept for no longer than is necessary. For other types of records (such as company, finance, and procedural records) certain company or accounting laws will apply.

Where no law applies, best practice standards, and the guidance below must be followed. All areas of the business must have in place robust procedures for the secure retention and safe disposal of information that protect the confidentiality of the business, residents, and staff.

Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this Policy or Record Retention Schedule. As such, The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Examples may include duplicates of originals, preliminary drafts, informal notes that do not represent significant steps or decisions, books, periodicals, manuals, materials retained for reference purposes, and spam or junk mail.

Personal Information – data from which living individuals can be identified.

Personal information must be as accurate and up to date as possible and processed only for the reasons given to those about whom the information relates. It must not be kept indefinitely (unless there is a “Legal Hold” in place or specific law requiring us so to do) nor on a “just in case needed” basis,

Personal information will be retained whilst there is an on-going relationship with the legitimate “data subject” such as a resident, member of staff or persons with whom we have entered into a contract. It will also be retained after the business relationship has ended for a limited time period as described in our Record Retention Schedule.

Other company or business records

Not all information held is personal data. Other records of appreciable value to the company exist and will include Information relating to business processes, company incorporation, contracts of service, finance and taxation, legal and regulatory affairs, land and property, insurance, and many other things. This information will only be retained for as long as it is needed for clear business or legal reasons. This will vary according to the type of record and the specific law, regulation or industry best practice that applies, as described in our Record Retention Schedule.

Hard-copy (paper) storage

Hard-copy storage and filing systems are to be kept to a minimum and, where practical, be set up to include a separate date tracking record, either hard-copy or separate system-based such as Microsoft Word or Excel; this will enable information to be destroyed more easily on the expiry date.

Certain information has to be retained in hard copy format for legal reasons – for example documents signed and sealed as a deed. As a general rule, as much information as possible is to be scanned or saved into structured computer systems. This is the most secure way of storing information, as daily back-ups are made.

Electronic storage

All information that is stored electronically will be retrievable as necessary in an appropriate format that can be read by those exercising their right to access information about them.

Disposal of Information

The Record Retention Schedule referred to in the “Cross References” section below, details the types of documents or records that are to be processed as a business and the length of time this information should be retained. It also sets out the minimum storage standards for each record type, both hard-copy and electronic. For ease, this has been set out by business area/function as well as by type of information, so that users can sort the schedule according to needs. Our Data Owners within the business line are responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction.

When records are no longer required and do not have archival value, they must be securely destroyed or deleted. All copies of the information should be destroyed at the same time, both digital and physical.

In all cases, confidential hard-copy information that is no longer required will be disposed of using confidential shredding bins or bags. These are provided in all offices and are the most secure and environmentally friendly method of disposal. Documents stored on electronic systems should be deleted, including back-ups, and not overwritten. Non-confidential data may be destroyed by recycling.

Permanent or Life of Company Preservation

Any information which is selected for preservation should be clearly marked to ensure it is not destroyed accidentally.

Legal Holds (Litigation Holds) and other Preservation Circumstances

A legal hold (sometimes known as a Litigation Hold) is the process of preserving all forms of information relevant to legal proceedings. A legal hold might be required if information we hold relates to a Public Inquiry or if it pertains to litigation that the organisation is involved with.

The Legal team will issue advice if a Legal Hold is to be put in place. When a Legal Hold is in place, there is a freeze on the destruction or deletion of any relevant material held by the organisation. In this instance, the relevant information must be clearly marked as such so it is not accidentally included in any scheduled disposal or deletion. Destruction may begin again once the Legal Hold has been lifted.

If you believe, or the Legal or Governance Team informs you, that certain records are relevant to current litigation or contemplated litigation, government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until otherwise instructed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept. In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our partnership with another organisation or the replacement of our information technology systems.

Weeding

Not all information we create has long-term value. Our Record Retention Schedule does not include redundant, obsolete, or trivial (ROT) information. This should be destroyed periodically by each directorate as part of routine housekeeping.

'Weeding' does not apply to corporate records included in the Schedule, which should only be destroyed when they have reached the end of their retention period.

Weeding should be done on a regular basis to ensure that clutter does not build up over time. It is up to each team to decide a reasonable schedule for housekeeping, based on their resources and the amount of information they generate. The Senior Leadership Team should encourage weeding on a regular basis.

Weeding should cover all information the directorate stores, paper or digital, regardless of the system it is held on. This includes personal drives and desktops.

Below are common examples of information which are usually of limited value once they are no longer in use and can be weeded through housekeeping. This should not be seen as an exhaustive list.

Drafts - Draft documents lose value and can become obsolete once a final version has been published. However, on some occasions where significant changes or deviation have taken place, a draft may be retained to show how the final decision was made.

Emails - It is important that information assets are saved to shared spaces, to provide evidence of decisions made or action taken. Once a conversation has reached a significant point, any earlier emails from this chain can be deleted.

Duplicates – We should not retain duplications. Duplications can lead to multiple versions of information which can cause confusion.

Research Material – Whether developing policy or preparing to give advice, research material may be created or collected such as notes or copies of guidance from external organisations. The value of this information decreases once the final version has been created.

Limited Long Term Operational Value – Some information may be of importance for only a short period of time and then become redundant. This information should be weeded as soon as they are no longer required.

5. Equality, Diversity & Inclusion

This Policy (and associated Record Retention Schedule) sets out the retention requirements for all records of appreciable value to the company as well as the standards for their appropriate safe storage. As such, there is no obvious bearing on Equality & Diversity that could arise from employees adhering to this Policy.

6. Roles and responsibilities

The Executive Board are responsible for:

- Formally approving and ensuring their respective areas of the business abide by this policy and its principles and relevant legislation, supporting, procedures, and guidance.

The Chief Information Officer is responsible for:

- implementing the relevant technology and automation to assist compliance with this policy; and,
- the security of information produced, provided, or held. This includes ensuring that data is appropriately stored.

Company Secretary is responsible for:

- ensuring assurance controls for the appropriate retention and disposal of company documents and corporate data are in place,

Data Protection Officer is responsible for:

- ensuring that compliance with data protection legislation and good practice in relation to the retention of personal data, can be demonstrated,
- escalating concerns with compliance to Executive Board.

Data Protection Manager is responsible for:

- ensuring assurance controls for the appropriate retention of personal data protection are in place; and,
- providing guidance that support the appropriate retention and disposal of personal data.

Legal Team are responsible for:

- advising on the application of any “Legal Holds”.

The HR Team are responsible for:

- complying with this policy in relation to data relating to prospective employees, current employees, and past employees.

The IT and Information Security team are responsible for:

- ensuring fit for purpose network and internal systems security relating to this policy and the associated Information Security Policy.

The Facilities Management team are responsible for:

- ensuring the necessary processes to support the correct retention and disposal of physical documents via appropriate office equipment or facilities; and,
- managing the security and organisation of any off-site storage facilities.

The Data Protection Forum are responsible for:

- providing steerage for, and drive delivery in the business line of the correct retention and disposal of data; and
- appointing data stewards accountable for appropriate data retention and disposal in the business.

Certain Directors are designated “Data Owners”, set out in table 1 below, of specified data domains and associated data processes or transactions and accountable for:

- understanding how data is captured, maintained, retained, and disposed of;
- being clear on why we need it, what is it used for, and who uses it;
- driving fit for purpose information security, retention, and disposal; and,
- authorising the destruction or disposal of information as required.

Line Managers are responsible for ensuring the departments and staff under their control comply with this policy and relevant laws in the responsible retention and disposal of all company and personal data. This includes ensuring staff are aware of the Record Retention Schedule referred to in the “Cross References” section below and setting up arrangements to securely dispose of or delete anything that should no longer be retained.

ensuring the appropriate retention and disposal of personal and company data within their specific business areas;

Table 1 below sets out staff members designated as “Data Stewards who have specified data processes or transactions, and are responsible for:

- ensuring the appropriate retention and disposal of personal and company data within their specific business areas;
- guiding business users in adherence to this policy;
- de-duplication of documents and data to achieve a single version of the truth;
- determining how and where data should be stored, access controlled, and kept secure; and,
- responding to staff queries about data retention and disposal.

- Table 1 – Data Owners & Stewards

Data Domain	Data Owner	Data Steward
Property/Asset	Senior Director Property Services	Interim Assistant Director Asset Performance & Intervention
Customer/Tenancy	Director Customer Services	Head of Customer Quality & Assurance
Repairs & Operations	Director of Repairs & Estates	Interim Assistant Director Asset Performance & Intervention
Finance	Director Financial Services	Head of Finance Services
People/HR	Director People & Culture	Head of People Operations
Governance & Strategy	Director Governance & Compliance, supported by Director Strategy & Policy	Head of Governance
Development	Director Development Delivery	Interim Senior Systems & Data Manager
IT	Director Infrastructure & Service Delivery	TBC

All staff, managers, and board members are responsible for:

- referring to the separate Record Retention Schedule referred to in the “Cross References” section below, and securely disposing of, or deleting, anything that should no longer be retained.
- abiding by and adhering to this policy at all times and as required by their contracts of employment; and,
- immediately reporting any known or suspected violation of this policy, or data protection breach, or via the documented breach reporting procedure on the company intranet site(s), or to the Data Protection Officer Inbox (dataprotectionofficer@paradigmhousing.co.uk) managed by the Data Protection Manager.

7. Compliance/Key Performance Measures

Mandatory training on data protection is required to be undertaken by all new starters and annually by all employees. Records of data protection training are kept up to date and maintained by the L&D team.

An annual data clearance exercise commenced in 2022 and is being continually encouraged as an annual weeding exercise. Clear desk procedures and the minimisation of stored physical data are also encouraged.

There is a dedicated email address dataprotectionofficer@paradigmhousing.co.uk for staff to raise data queries relating to personal data retention. Customers can make data erasure (right to be forgotten) requests by phone or email. This is supported by documented procedures, managed by the Customer Information Team, for responding to such erasure requests as well as for complying with other data subject rights including restricting, or objecting to processing.

An approved Record Retention Schedule is in place relating to all types of company data (both personal and other) and to guide staff in retaining data only as long as is needed, or as relevant law allows. It also sets the minimum standards of storage for each record type, both hard-copy and electronic.

The Data Protection Forum will continue to drive sound data governance via appointed “Data Owners/Stewards” as well as minimising both hard-copy and electronic data held.

8. Related Policies, Procedures and Key Documents

Key Policies and Documents

- Data Protection Policy
- Information Security Policy.
- IT User Policy.

Supporting procedures, processes and guidance documents

- a. Record Retention Schedule
- b. Information asset register/data inventory.
- c. Subject Access and Privacy Rights Requests procedures.

9. Version Control

Version control			
Date	Version	Approved By	Details of Amendments
June 2026	V1	Executive Board	Review following the SettleParadigm Merger to

			amalgamate and align respective and relevant policies from both organisations and align with National Housing Federation Guidance.
--	--	--	--