Stockport Homes Group

One team, transforming lives

RECORDS MANAGEMENT POLICY

16 January 2018

Prepared by:	Assurance Manager
Date effective from:	16/01/2018
Policy approved by:	Assistant Chief Executive
Review Date:	16/01/2021

EIA Required?	☐
EIA Completed?	☐
Revision number:	1
Lead officer:	Assurance Manager

1 INTRODUCTION

1.1 An effective approach to records management is essential for Stockport Homes Group to meet certain statutory requirements but also to ensure a culture of excellence in Information Governance (IG).

1.2 It is important to have an understanding of the records which exist within the Group, how long these need to be retained for and the reasons for this. This will enable processes to be followed when the retention end date is arrived at, ensuring they are disposed of securely when the time arises.

1.3 Storing documents which are no longer required by the Group wastes money and resources, becoming a burden on the Group rather than an asset. By having an effective records management culture, SHG will ensure it is only retaining those records for which there is a purpose for them to be kept.

1.4 This policy ensures legislative / regulatory requirements are met but that best practice in this area is also implemented across the organisation.

2 BACKGROUND

2.1 The organisation's Information Governance Policy sets out how the requirements of the following pieces of legislation will be met:

- Data Protection Act (DPA) 1998[1]
- Freedom of Information Act (FOIA) 2000
- Environmental Information Regulations (EIR) 2004

2.2 Each of these statutes gives people access to information. The FOIA and EIR give people an access to corporate information to assist with transparency and governance, whilst the DPA gives people a right to access personal data held about them.

2.3 It is important to note that in May 2018, the General Data Protection Regulation (GDPR), which is a piece of EU legislation, will become law in the UK. Furthermore, the UK will introduce a new Data Protection Bill (DPB) to replace the current DPA 1998. It will be necessary for SHG's operations to comply with these new pieces of legislation.

2.4 Under the existing FOIA 2000, a Code of Practice was issued under Section 46 and furthermore the DPA sets out, via the fifth principle, that *"personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes*".

2.5 This means that data should be retained where a relevant statutory time limit exists, or where there is a demonstrable organisational requirement for retention. It is imperative that managers are aware of the records which exist

[1] Which will be replaced by the General Data Protection Regulation (GDPR) from May 2018

within their business area and understand the corresponding legislation related to those records which may enforce a requirement to retain. Assistance is available from the Assurance Team if managers need support in this.

2.6 Furthermore, there are a number of other pieces of legislative / regulatory / best practice requirements which must be considered as part of a records management solution. These are:

- Limitation Act 1980
- Other key legislation related to service delivery
- FSA regulations
- HMRC requirements
- Guidance from professional bodies such as CIPD
- ISO standards
- Sector best practice
- Requirements of the GDPR (from 2018)

3 WHAT IS RECORDS MANAGEMENT?

3.1 Records management is about **controlling records** within a comprehensive regime made up of policies, procedures, systems, processes and behaviours.

3.2 Such a framework ensures that reliable **evidence of actions and decisions** is kept and remains available for reference and use when needed, and that the organisation benefits from effective management of one of its key assets: its records.

3.3 It governs the practice of anyone who **creates or uses records** in the course of their daily working life and ensures that appropriate attention and protection is given to all records held by the organisation.

3.4 Features / benefits of a good records management framework include:

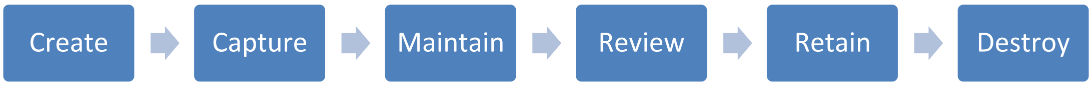
- Safeguarding the authenticity, reliability, integrity and useability of the record
- Service delivery is maintained and business can be conducted as planned (using minimum amount of information)
- Evidence is kept of business activities / transactions (accountability)
- Information assets are secured (authentic / reliable records)
- Informed decisions can be made as the right information is available at the right time
- Current and future business / stakeholder needs can be accommodated
- Compliance with regulation / legislation / best practice
- Protection of people and information
- Better use of resources and more efficient operational processes
- Openness and transparency
- Records can be easily retrieved (in an efficient and effective manner)
- Records are created once, accessible in one location and held electronically where possible

- Creates a corporate memory for the organisation and its stakeholders
- Consideration given to anything needing to be preserved indefinitely
- Enables the organisation to respond effectively to a business continuity event
- Protect the organisation fully in the event of any litigation action
- Track policy changes / evolvement over time
- Provide an audit trail of decisions / action taken

4 WHAT ARE RECORDS?

4.1 A “document” is a piece of recorded information. A **“record” is evidence of a business activity / transaction**. There is a subtle difference and this policy is intended to provide a framework for managing **records**.

4.2 A record should be **accurate, reliable, ordered, complete, useful, up to date and accessible**. Each record has a lifecycle. The following stages should be considered for each record:



4.3 When a record is created / received / captured, it is preferable that there is a process in place to register it, classify it, set access and security parameters (including how the record will be transmitted between systems / users), assign a retention period to it and determine the media by which it should be retained. Work is ongoing to further embed this within the Group.

4.4 When a record is reviewed, consideration should be given to whether it should be retained for longer, destroyed immediately, transferred to another organisation / location or media. Where necessary, advice should be sought if a manager is unsure whether a record needs to be retained, or not.

5 ROLES AND RESPONSIBILITIES

5.1 Assistant Chief Executive

5.2 The Assistant Chief Executive is the lead officer and has overall responsibility for Information Governance and IT services within the Group. These functions are imperative to having an excellent approach to records management.

5.3 Directors and Heads of Service

5.4 All Directors and Heads of Service have a responsibility to implement this Policy within their Directorates / Teams. They are responsible for ensuring that their service managers and team members are familiar with this policy and that working practices are embedded to deliver an excellent approach to records management.

5.5 **Assurance Manager**

5.6 The Assurance Manager takes the role of the Data Protection Officer within the organisation. It is their responsibility to embed an information governance framework which delivers compliance against legislative requirements regarding information management.

5.7 The Assurance Manager will ensure there is in place a suite of information governance policies, procedures and guidance for managers to utilise in their own service areas.

5.8 The Assurance Manager is not expected to have a detailed understanding of the operational requirement of all records within the organisation; this is the responsibility of service managers.

5.9 **Head of IT**

5.10 The Head of IT (and the wider IT Team) will work with the Group to design and deliver a range of corporate IT solutions to the Group which allow effective service delivery and enable this policy to be successfully implemented.

5.11 **Service Managers**

5.12 It is the specific responsibility of managers to understand the records which are created, held and processed by their team in relation to delivering services.

5.13 They must familiarise themselves with the type and volume of records to enable effective direction to be given regarding their retention (or destruction) requirements.

5.14 Managers are Information Asset Owners and need to ensure they dedicate sufficient time and resource to enabling effective records management within their service / team.

5.15 Managers are responsible for ensuring that all records within their service area are managed in accordance with this policy, cascading messages to staff as required and to seek advice where necessary.

5.16 **Team Members**

5.17 Team members within the Group are required to adhere to this policy, implement agreed working practices, understand the importance of effective records management and raise any issues with their own manager.

5.18 Team members are key to ensuring an effective and embedded culture in relation to records management and should raise any issues which they identify with their manager.

6 RETENTION SCHEDULE

6.1 The retention schedule is provided as a separate document[2]. This is intended to set out *key principles* around retention periods for different types of records. This approach will ensure the retention schedule remains fit for purpose as the organisation grows and diversifies.

6.2 **It is not intended to be a definitive list for each individual team. It should be viewed as a 'live' document which can be updated as required.**

6.3 Records held by SHG may be called upon in the future to provide evidence of event / actions / decisions which were taken in the past. It is not acceptable to have a "keep everything" approach, as under DPA, the Group needs to be able to justify why it is processing (retaining / storing) such information.

6.4 The majority (but not all) of potential legal claims are statute barred on the expiry of six years[3]. This means that in general, it is considered prudent to keep records for six years from the date when the subject matter was completed, as this is the time frame in which civil proceedings can be brought against the organisation. However, records may be retained for longer where specific criteria apply[4], or for shorter periods where the record has ceased to be of value to the organisation, and there is no reasonable justification to retain (as retention is still processing).

6.5 Where a record is to be produced in court, it must be authenticated as a true copy of the original. Ordinarily, this is the case where the organisation has the original hard copy and can therefore certify that the copy is true. Each service will therefore need to consider the following:

- How hard copy documents have been transferred to electronic records to support a paperless working environment and flexible working
- Whether or not it is likely that these documents will be required to support litigation or as legal proof (and whether a hard copy is to be retained, in archive, as well as electronic versions)
- If the risk of documents being required for litigation is small or zero, whether the hard copies can then be disposed of.

6.6 Where managers feel there are items which should be added to the Retention Schedule, they should inform the Assurance Manager who can make such amendments, as required.

[2] This is available on the HOG (Stockport Homes intranet site)

[3] According to the Limitations Act 1980

[4] An example of this is when the record is the subject of a request for information or being used in litigation proceedings. This should not be disposed of until the access request has been concluded.

7 STORAGE OF RECORDS

7.1 There are a variety of ways in which records can be stored. The retention period and type of record will be key factors in deciding what the most appropriate storage medium is.

7.2 Consideration should be given to the storage environment, the media to be used, the physical location of the records, handling procedures, protective materials and access and security requirements.

7.3 Where a record is one of historical (or other) interest / value, there may be a requirement to retain this record permanently. This should be clearly visible on the record itself. It is advisable that these records are deposited in a third party archive facility for preservation.

7.4 Managers should seek advice, as necessary, if they are unsure about the fitness for purpose of their storage solutions.

8 DESTRUCTION OF RECORDS

8.1 After the end of the retention period, most records will go on to be destroyed.

8.2 The destruction of records is a permanent act and so the decision must be made correctly, after considering all options / impacts. It is good practice for the manager to record the decision to destroy and what records have been destroyed each time. Please see appendix one for a records disposal form.

8.3 Disposal records should state what records have been disposed of, the date and the reason for the disposal. This is to ensure the organisation can evidence the disposal in the event of a future dispute, evidencing why the record is no longer available.

8.4 Many of the organisation’s records may contain personal / sensitive / confidential information and so it is imperative that these are destroyed securely. This is to ensure that the confidentiality of the data is safeguarded throughout the records lifecycle and also to ensure compliance with the data protection principles.

8.5 The following practices are recommended for different types of media:

- Paper records can be securely destroyed via use of confidential waste bins, shredding, pulping or incineration
- CDs / DVDs must be shredded using a disc shredder
- Electronic files should be deleted from main systems and any archives, test systems or back-ups held.

8.6 Where an external contractor is used for disposal / destruction of records, the relevant due diligence should be undertaken of the organisation to ensure they are competent and reliable. They must sign confidentiality agreements as part of the contract and must provide written proof of destruction.

9 MONITORING OF COMPLIANCE

9.1 It is everyone’s responsibility to ensure that records within the Group are managed in accordance with this policy.

9.2 The Assurance Manager will be responsible for monitoring compliance with this policy.

9.3 Consideration will be given to the use of Internal Audit (or other independent body) to provide independent assurance around the organisational approach to records management.

10 EQUALITY IMPACT ASSESSMENT

10.1 The Equality Impact Relevance Screening has concluded that an Equality Impact Assessment is not required.

11 OWNERSHIP, MONITORING AND REVIEW

11.1 This policy is owned by the Assurance service although there are clear roles and responsibilities for others, as described above.

11.2 The policy will be monitored on an ongoing basis and reviewed every three years, or when there is a major change in legislation or best practice.

Appendix One:
Records Disposal Form

Directorate	
Service / Team	
File Number / Reference / ID	
Description of records	
Storage medium	□ paper □ video tape □ CD □ database □ floppy disk □ electronic file □ other (please state) ……………………..
Date range of records destroyed	
Date of destruction	
Destruction method	□ shredding □ incineration □ pulping □ other □ deletion (please state) …………………….
Name and job title of person destroying the records	
Name and job title of person authorising the destruction (Senior Manager)	
Any additional notes	