RECORDS MANAGEMENT POLICY

Document history

Date	Version	Author	Changes made
Feb 21	1.0	Sally Turnbull	Initial version

Approvals

Name	Signature	Role/Title	Date
Stuart Field		ICT Manager	Jan 21
James Rutter		ICT Manager	Jan 21
Gavin Ramtohal		Head of Legal Services and DPO	Jan 21
Sally Turnbull		Information Governance Manager	Jan 21
JSCG			

Document Filename and Location:

Filename: Surrey Heath Records Management Policy

Format	Version	Filepath	Owner
Draft	Draft 0.1		Sally Turnbull
Published			

Format	Version	Filepath	Owner

1. INTRODUCTION

1.1 Information, in all its forms, whether electronic, paper-based or staff knowledge, is Surrey Heath Borough Councils (SHBC) second most important resource after our people. Records Management is at the heart of the way in which we deliver service to the public. If we do not have consistent and accurate records we cannot optimise our efficiency or measure the improvements; in order to achieve this, our records should be:

(a) **Available** - Records will be available to those who need it, and who have the permissions to view or use it. We will avoid information overload and target information where it is needed.

(b) **Accessible -** Our records should be clearly identified and easily found when needed by anyone who needs to access it.

(c) **Electronic** - Our records and documents will be stored electronically. Over time, we will evolve our policies such that we will endeavour to only keep paper records where there is a legal requirement to do so.

(d) **Secure** - Records will be protected and retained as appropriate. We will record the confidentiality of information. Non confidential information will be openly published.

1.2 All records created and received by the Council, and its external service providers where they are processing information on the Council's behalf, are the property of the Council, and must not be used for any activity or purpose other than official Council business.

1.3 Failure to manage records properly within SHBC exposes the council to a significant financial, legal, confidentiality, public relations and potentially manpower-shortage risk.

2. PURPOSE

2.1 This policy sets out the Council-wide policy for records management standards that should be adhered to by all SHBC staff working with SHBC records including permanent and temporary employees including those who are agile working, working off-site and working jointly with partners, ~~elected members,~~ volunteers, contractors, secondments and work experience placements.

2.2 The Records Management Policy is about how Surrey Heath receives, creates, communicates, stores, uses and distributes the information we need to deliver our services and corporate objectives.

2.3 This policy applies to all the Council's information and data sets in all formats - paper, electronic (including graphical, audio, photographic and video files) and, so far as feasible, staff knowledge, including those that the Council creates, holds on behalf of others or shares with third parties or partner organisations. All information, records and data sets including emails need to be stored in a manner that allows effective retrieval and allows the relevant retention rules to be applied.

2.4 The Policy will add value to the information resources used by the authority and will promote efficiency. It will show customers and citizens that the Council has a commitment to providing high quality information and takes its role as the custodian of information seriously.

3. OBJECTIVES

3.1 The objectives of the Records Management Policy are:

(a) To instil an understanding of the importance, and an appreciation of the potential, of effective records management.

(b) To help develop awareness, understanding and to promote the application of good practice in handling information, and develop efficiency and effectiveness in this area.

(c) To support SHBC's ambition to improve processes, to improve customer services, to become more efficient and to reduce costs.

(d) To meet legislative and regulatory requirements and apply best practice.

4. RELEVANT LEGISLATION

4.1 Good records management must be managed in accordance with current legislation and existing professional standards. These include the following;

- Local Government Act 1972
- Local Government (Access to Information) Act 1985
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulation 2004
- Re-use of Public Sector Information Regulations 2015
- Public Records Act 1958 and 1967

- Human Rights Act 1998
- Lord Chancellors Code of Practise for Records Management
- In addition certain records will be subject to other legislation covering their subject area.

As well as key legislation there are useful guidance and procedures that should be consulted to ensure good records management these include;

- ICO guide to 'Records Management and Security'
- Cabinet Office 'Data Handling Procedures in Government'
- LGA 'Data and Transparency'

5. RELATIONSHIP WITH EXISTING POLICIES

5.1 This policy should be read in conjunction with the following related polices and guidance's;

- Information Security Policy
- Data Protection Policy
- Information Governance Strategy
- Email Guidance
- Corporate Style Guide
- Disciplinary Policy
- Offsite Working Policy

6. KEY DEFINITIONS

6.1 A "Record" is information held by the Council that relates to a specific topic, area of work or an individual. The record can be held in paper or electronic format

6.2 'Personal Data' is information that relates to an identified or identifiable person who could be identified, directly or indirectly based on the information.

6.3 "Records Management" is the planning, control, organisation and training activities relating to the creation, distribution, utilisation, storage, retrieval, maintenance, protection, preservation and final disposal of all types of records required for the conduct of the Council's activities

6.4 A "Records Retention Schedule" is a policy that defines how long records must be kept and provides disposal guidelines for how data items should be discarded. Records retention schedules are determined by the record type and the business, legal and compliance requirements associated with the data.

7. ROLES AND RESPONSIBILITIES

7.1 Corporate Management Team (CMT)

Are responsible for ensuring that the business areas they have responsibility for have processes and procedures in place that support this policy.

7.2 Data Protection Officer (DPO)

Is responsible for setting strategic direction and ensuring that policies and processes are in place for the safe management of information. The DPO is supported in this role by the Information Governance Manager.

7.3 **Information Asset Owner (IAO)**

Are responsible for ensuring appropriate information management practices including access controls and record retention and destruction are in place for their information assets (electronic and paper).

7.4 **Information Governance Manager**

Is responsible for working with the DPO to set strategic direction, ensuring that policies and processes are in place for the safe management of information.

7.5 **ICT**

Is responsible for providing and maintaining the secure infrastructure to enable information users to have access to information they require to deliver their services. In conjunction with Information Asset Owners and information users, the ICT Service will work towards the automation of the Council's archiving and records retention policy using cost effective and approved technology solutions.

7.6 **Line Managers**

Are responsible for ensuring their staff are aware of their information management responsibilities and arrangements for access to information, and that staff are appropriately trained or experienced.

7.7 **All staff**

All SHBC staff, ~~elected members,~~ contractors, consultants and agents ("information users") are responsible for managing records in accordance with this policy and related procedures. When leaving the Council, all staff must ensure that key Council records for which they are responsible remain accessible.

8. CREATION OF RECORDS

8.1 Records should be created and captured in a timely manner. This should either be done by someone who has direct knowledge of the event or transaction, or generated automatically as part of a routine operation.

8.2 Where appropriate, when creating records current corporate templates should be used for all documentation both physical and electronic.

8.3 Website content should be produced in compliance with The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

8.4 Records should have meaningful titles and where applicable include indexes/metadata so that they can be retrieved quickly and efficiently

8.5 To reduce duplication which can lead to incorrect records being updated or available, records should be centralised with version control and dated.

8.6 Records should be complete and accurate enough to allow staff (including any successors) to undertake all actions for which they are responsible.

8.7 The creator of the record is responsible for ensuring that it is accurate, of good quality, relevant, up-to-date, and if includes personal, sensitive or confidential information it is secure.

8.8 ICT should ensure appropriate backup arrangements are in place for electronic records (including restoration of backups and disaster recovery if electronic records are damaged).

9. STORAGE

9.1 To maximise efficiency, reduce costs, enable appropriate access and sharing and minimise risks, records must always be stored securely in corporate repositories, these include:

(a) **Filing cabinets**, physical storage accommodation for records should be clean and tidy, to prevent damage to the records, and securely protect against unauthorised access.

(b) **Microfiche or archiving system** (Alchemy) If applicable

(c) **The internet and intranet**. Both are extensive and contain a great deal of corporate information, including Committee reports and agendas (via the ModernGov platform), and a range of services and e-forms.

(d) **Microsoft Office and outlook**. All staff use the corporate systems, and calendars are generally open. Use of e-mail helps to share information but email should not be use as a storage of records instead records should be moved to the relevant service system or Box folder.

(e) **Box**. Each staff member has their own personal box folder, information of a confidential or sensitive nature should be stored within your own box folder and should be password protected. Only SHBC related data must be stored on Box. All services areas have their own box folder. Some of these are made available for corporate use either generally or on request while others are held and used locally within the service. The centralised filing structures in Box enable services to share documents and improve the security of our records. Box governance standards including access management, retention periods and classifications should be set when setting up box folders especially when the information being stored is of a personal or confidential nature.

(f) **Specialist Software Systems**. Specialist systems are used in some areas – these include; Northgate in Revenues and Benefits, Uniform in Planning, Licensing, Enforcement, Tree Protection, Listed Building and Land Charges, Civica in Finance, Xpress in Electoral Registrations and iKen in Legal. Access to these systems should be on a need to know basis and records should be managed in line with this policy.

(g) **Customer Relationship Management (CRM).** The Plan Alpha CRM system holds documents and records of all customer contacts through Customer Services, together with additional information from some contacts through other services. Access to Plan Alpha should be on a need to know basis and records should be managed in line with this policy.

(h) **Geographical Information System (GIS)**. We have established a corporate platform for mapping information, with integration into a number of key databases, and browser-based delivery through the Xmap mapping services. Our Local Land and Property Gazetteer is the definitive source for addressing in the council and publishes nightly address change updates to the National Land and Property Gazetteer. Access to the GIS system is managed by ICT.

(i) **USB drives / memory sticks and other removable media**. In the majority of circumstances ICT will no longer supply removable media such as USB sticks to staff as they are no longer required. Additionally ICT monitoring systems will prevent their usage on SHBC supplied equipment. Removeable medias must not be used for permanent storage of records. If you are required to transfer records, on most occasions, you are advised to use the sharing tools within Box

which are secure and timely. Only removable media supplied by ICT Services should be used with SHBC systems, all removeable media supplied by ICT are encrypted to the correct standard.

9.2 Avoid storing duplicates (e.g. avoid paper/electronic overlaps, e.g. store a single copy of electronic information to be shared through use of box links) and routinely destroy unnecessary information (in accordance with the corporate retention schedule);

9.3 If the record being stored includes personal or sensitive data additional security measures must be taken to ensure that only staff that need to know have access to the data, this will include, setting access controls to specific staff, ensuring password are set to access the records and for physical records ensure they are securely locked away. Additionally, Box sharelinks can be set to expire a certain number of days after they have been created.

10. RECORDS RETENTION AND DISPOSAL

10.1 The retention and disposal schedule ~~that are~~is maintained by the IAO in each service area and centrally managed within the Information Governance Department, helps the Council to meet its statutory obligations to ensure that information is retained for the correct period of time and then disposed of appropriately. It is unlawful to retain information for longer than necessary.

10.2 Electronic information should be treated in the same way as physical information; therefore, electronic information, where the system allows, must be disposed of once it has reached its set disposal date.

10.3 Each department/section should have a records retention schedule/policy in place which will outline the appropriate retention periods for records. These retention periods should be based on legislative requirements and common practice in the sector. The retention periods listed in the schedule are the minimum length of time which the data, information and records must be kept. retention schedules should be regularly reviewed (at a minimum every three years).

10.4 Where systems have the functionality to set retention periods on records or groups of records, it is recommended that an intended disposal or review date is captured when creating the electronic records.

10.5 IAO will review records in accordance with the retention schedule, when they are no longer required for on-going business or specific legal or regulatory purposes, records will be securely destroyed.

10.6 At the end of the retention period, the record should be assessed to see whether it ought to be selected for permanent preservation, e.g. if it is of historical interest. Such records should either be retained by the Council or be offered to the Surrey History Centre for archiving

10.7 Records that could be subject to a Freedom of Information or Data Protection request must not destroyed unless the approved retention period has been met.

11. CLASSIFICATION

11.1 Where appropriate, the National Protective Marking Scheme classifications should be used. This provides for unclassified information and 3 levels of classification Official, Secret and Top Secret. In most cases local government information will fall into the lower category of UNCLASSIFIED. It is not necessary to mark each

document/email if it is official. If it contains sensitive/personal information you may wish to classify it Official – Sensitive in the subject field of the email.

12. BUSINESS CONTINUITY

12.1 Information Asset Owners are responsible for identifying the data, information and records (regardless of the media in which they are stored) which are considered to be business critical and to ensure that the business critical elements are included in individual service unit business continuity plans.

12.2 It is the responsibility of ICT to ensure that backups are created to the agreed standards and to establish an effective back-up restoration regime to ensure that when back-ups need to be restored they remain fit for purpose.

13. DATA PROTECTION, PRINCIPLES OF RECORDS MANAGEMENT

13.1 Information which is subject to security controls i.e. personal, sensitive, confidential data, will be identified, and will be held and used in accordance with a Data Protection regime appropriate to the nature of the information.

13.2 Public information will, so far as reasonably possible, be made available without charge.

13.3 Information will be retained, archived and disposed of according to a records retention schedules.

13.4 The Council has an Information Asset Register (IAR) that identifies the information assets owned by the Council. The IAR is subject to an annual review and any risks identified will be reported to the Information Governance Manager.

13.5 Email and c:\ drives will not be used to store council information, staff should only store case work and other council information in the location agreed by their IAO this will usually be a specific system used by that department or Service Area or another corporately agreed location within the Council network.

13.6 The IAO will ensure that where new systems that store personal data or any sharing of personal data with third parties is to be undertaken a Data Protection Impact Assessment is completed before the sharing can take place.

13.7 Where records are being shared or systems accessed by third party data processors, contracts with the appropriate Data Protection and records management clauses regarding the agreed and approved methods of information handling are included.

14. MONITORING AND REVIEW

14.1 This policy will be reviewed when required or at the minimum at least every 5 years. The Information Governance Manager will regularly monitor compliance with the policy procedures and guidelines making any amendments and improvements as necessary.