DARTFORD
BOROUGH COUNCIL

RECORDS MANAGEMENT POLICY

1. Introduction

(a) This Records Management Policy (the RM Policy) sets out a corporate policy and framework for the management of records held by the Council and covers:

- the requirements that must be met for records of the Council to be considered as proper records of the activities of the organisation;
- the requirements for systems and processes that deal with records;
- the quality and reliability which must be maintained to provide a valuable information and knowledge resource for the Council;
- its place within the strategic and policy framework of the Council;
- the requirements governing records' identification process;
- the requirements for the preservation of information;
- the requirements for reviewing this RM Policy and ensuring implementation/compliance throughout the Council.

(b) The benefits of an effective records management are:

- support for the Council's decision making processes and activities;
- protecting business critical records and improving business resilience;
- ensuring information can be found and retrieved quickly and efficiently;
- complying with legal and regulatory requirements;
- accountability;
- reducing risk for litigation, audit and regulatory bodies' investigations;
- minimising storage requirements and reducing costs.

(c) Information is a key business asset and its proper use is not simply an IT issue. There are clear lines of accountability throughout the Council together with a programme of staff awareness raising, which clearly sets out the expectations of staff.

(d) In this RM Policy, '**record/s'** is any recorded information in any form, including data in computer systems created or received and maintained by or on behalf of the Council in the transaction of business or the conduct of affairs and which:

- informs, supports, provokes or evidences decision-making or activity by or on behalf of the Council or;
- is required to be kept by legislation, or for audit or other organisational purpose; or
- safeguards the position of the Council and/or its stakeholders;
- requires to be maintained/controlled i.e. managed,

regardless of medium (paper, microfilm, electronic, audio-visual, copies of publications etc.) and which are created, collected, processed, used, stored and/or disposed of by the Council, its employees and any other person/body/organisation acting for or on behalf of the Council as its agent.

(e) Legislation and codes of practice which affect the management of the Council's records include:

- Civil Contingencies Act 2004;
- Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004;
- Code of Practice on Records Management (section 46 FOI);
- Data Protection Act 2018;
- Data Sharing Code of Practice (ICO);
- Environmental Information Regulations 2004;
- Freedom of Information Act 2000 (FOI);
- General Data Protection Regulation ((EU) 2016/679) (GDPR);
- Human Rights Act 1998;
- Limitation Act 1980;
- Local Government (Access to information) Act 1985;
- Local Government Act 1972;
- Local Public Services Data Handling Guidelines (2012);
- Privacy and Electronic Communications (EC Directive) Regulations 2003;
- Public Services Network Code of Connection (CoCo).

2. Governance, accountability & transparency

While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. The Council is expected to put in place comprehensive but proportionate governance measures as follows:

- Determining what records should be created and retained by each Department through the establishment of a Data Retention & Disposal Schedule as set out in each Department's Information Asset Register;
- Publishing Privacy Notices for each Department explaining the legal basis for processing personal information, data retention periods and that individuals have a right to complain to the Information Commissioner's Office and seek judicial remedy if they think there is a problem with the way the Council is handling their data;
- Determining appropriate corporate systems for the retention of records which ensure all appropriate records and related data (metadata*) are captured into the system. These systems may be electronic or paper based, as appropriate;
- Ensuring that there is no unwarranted duplication between paper and electronic record collection;
- Retaining records to satisfy operational, legal and other needs;
- Developing appropriate retrieval aids such as classification schemes and indexes to facilitate the retrieval of records and information;
- Ensuring records are maintained in a safe and secure environment;

- Ensuring the physical security of Council premises and systems e.g. through the issue of staff ID cards, recording and/or accompanying all visitors wherever feasible, implementing a clear desk/clear screen policy, locked filing cabinets etc.;
- Ensuring records are retained for as long as required and no longer;
- Carrying out timely and appropriate destruction of records and information in conjunction with the Data Retention & Disposal Schedule referred to in each Department's Information Asset Register;
- Ensuring the secure disposal of information e.g. pulping, incineration or shredding;
- Ensuring that this RM Policy is aligned with the Council's Information Security Policy and recognise the importance of laptops and smartphones should be encrypted and/or used with Mobile Device Management software. The use of removable media including removable discs, CDs, USB memory sticks and media card formats should be avoided wherever possible. Where unavoidable, encryption should be used and the information transferred should be the minimum necessary to achieve the business objective;
- Ensuring that access to systems are restricted to those users that need it;
- Ensuring suitable password or similar protection particularly for sensitive personal data and financial data and access on a need to know basis;
- Wherever possible, ensure the bulk transfer of information is carried out via a secure network, secure file transfer using PGP or AES encryption;
- Carrying out penetration testing of the Council's ICT systems and network on a regular basis;
- Where appropriate, conducting data privacy impact assessments of new systems;
- Ensuring that new ICT systems are accredited to Government standards;
- Ensuring the implementation of business continuity plans and the undertaking of regular risk reviews of all processes and procedures;
- Ensuring robust breach detection, investigation and internal reporting procedures are in place for personal data breaches[1]. This will facilitate decision-making about whether or not the Council needs to notify the ICO and the affected individuals;
- Ensuring all staff are trained, updated and aware of their responsibilities; and
- Ensuring that the Council's suppliers, contractors, service providers etc. are mandated through contractual arrangements to adopt equivalent standards where they are contracted to process personal data on behalf of the Council.

** Metadata – data describing content, context and structure of records to allow them to be linked to the business process from which they were created*

[1] A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals

3. Officer accountability

(a) Data Protection Officer (DPO)

The Council is required under the Data Protection Legislation[2] to appoint a Data Protection Officer whose minimum tasks are to:

- inform and advise the Council and its employees about their obligations to comply with the Data Protection Legislation;
- monitor compliance with the Data Protection Legislation, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits;
- be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc.)

The Head of legal Services is the Council's appointed Data Protection Officer.

(b) Senior Information Risk Officer (SIRO)

The Strategic Director (Internal Services) is the Council's appointed SIRO who has responsibility for ensuring that the Council's IT systems' risk within the organisation is managed appropriately.

The SIRO's other responsibilities can be summarised as:

- owning the Council's overall IT Security Policy and IT risk assessment processes and ensuring they are implemented consistently by Information Asset Owners;
- advising the Management Team and the Audit Board on the information risk aspects of the Council's statement on internal controls/annual governance statement;
- reporting to the Audit Board on the effectiveness of the Council's' cyber security management processes;
- owning the Council's IT incident management framework.

(c) Directors

- support the DPO and the SIRO in their respective roles;
- ensure that written procedures for the management of records are established and followed within their respective Directorates to meet the requirements of this RM Policy.

(d) Services Managers/Information Asset Owners

- ensure the capture of records (both paper and electronic) that provide evidence of the Council's functional activities;
- ensure the requirements of this RM Policy are articulated in business plans and procedures/works instructions as necessary and appropriate;
- identify staff responsibilities to implement this RM Policy;
- establish record retention schedules for all areas of work;

[2] Data Protection Act 2018 (applying the GDPR)

- ensure that staff receive appropriate training to meet their responsibilities under this RM Policy;

(e) **Staff -** who create, use, manage or dispose of Council records:

- have a duty to protect them and to ensure that any information they add to the record is accurate, complete and necessary;

- abide by the Council's written procedures and departmental works instructions relating to records management.

4. RM Policy Statement

(a) Information is a corporate asset and the records of the Council are important sources of administrative, evidential and historical information. They are vital to the Council in its current and future operations, for the purposes of accountability, and for an awareness and understanding of its history and procedures. They form part of the corporate memory of the Council.

(b) In consultation with organisations which may be concerned with the management of records held by the Council on their behalf, the Council will create, use, manage and destroy or preserve such records in accordance with all statutory requirements and/or organisational specific requirements.

(c) Systematic records management is fundamental to Council efficiency. It ensures that the right information is:

- captured, stored, retrieved and destroyed or preserved according to need;
- fully exploited to meet current and future needs, and to support change;
- accessible to those who need to make use of it,

and

that the appropriate technical, organisational and IT and staffing resource elements exist to make this possible.

(d) The Council's records management system aims to ensure that:

- the record is present;
- there is no unnecessary duplication of the record;
- the Council has the information that is needed to form a reconstruction of activities or transactions that have taken place;
- it is possible to locate and access the information and display it in a way consistent with initial use;
- the record can be interpreted;
- it is possible to establish the context of the record: who created it, during which business process, and how the record is related to other records;
- the record can be trusted;
- the record reliably represents the information that was actually used in or created by the business process, and its integrity and authenticity can be demonstrated;

- the record can be maintained through time;
- the qualities of accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of formats.

5. Policy Framework

This RM Policy may be merged with other general corporate policies or strategies or kept separate.

(a) Following Best Practice

- records should be managed in accordance with relevant codes of practice for records management such as ISO 15489, which provides an overall guide to best practice in records management of the Council's e-business strategy;

- electronic records will underpin e-business providing records for business use, corporate knowledge management and evidence-based policy making, and evidence for accountability and historical use.

(b) Freedom of Information

The formation and maintenance of records will adhere to procedures under the Freedom of Information Act 2000 and the associated code of practice.

(c) Data Protection Legislation

Protecting personal information is a legal requirement under the Data Protection Legislation with a view to protecting the privacy of the individual in relation to the personal information the Council may hold about them.

The Data Protection Legislation establishes key principles that govern the collection, use and handling of personal information and provides individuals with important rights.

To meet its obligations under the Data Protection Legislation, the Council:

- has defined and allocated records management responsibilities;
- has approved and published an appropriate records management policy. This is subject to a regular review process;
- has identified records management risks as part of a wider information risk management process;
- incorporates records management within a formal training programme. This comprises mandatory records management induction training with regular refresher material, and specialist training for those with specific records management functions;
- has established written agreements with third party service providers that include appropriate information security conditions;
- ensures the protection of personal data that is accessed by suppliers and providers;
- carries out periodic checks on records' security including compliance with records management procedures;

- has minimum standards for creation of paper or electronic records and has established processes to ensure that there is a lawful/legal basis for processing personal data prior to collecting it;
- has identified manual and electronic record keeping systems throughout the organisation and actively maintains a centralised record (Information Asset Registers) of those systems;
- has processes in place to ensure that personal data that is collected is accurate, adequate, relevant and not excessive. Routine weeding is also carried out to remove any personal data or records that are no longer relevant or out of date;
- has appropriate measures in place for the transfer of electronic records offsite to protect personal data from loss of theft;
- stores paper and electronic records securely with appropriate environmental controls and higher levels of security around special categories of data (i.e. sensitive personal data);
- restricts access to records storage areas in order to prevent unauthorised access, damage, theft or loss. Access is role based in line with the principle of least privilege and checked regularly;
- has a process to assign user accounts to authorised individuals and to remove them when no longer appropriate. Such access is granted on the basis of least privilege with appropriate access controls in place;
- has business continuity plans in place. These identify records that are critical to the continued functioning or reconstitution of the organisation in the event of a disaster. Data that is stored electronically is routinely backed-up to help restore information in the event of disaster;
- has a retention and disposal schedule in place which details how long manual and electronic records will be kept for;
- has defined confidential waste disposal processes in place to ensure that records are destroyed to an appropriate standard once a disposal decision has been made.

(d) **Environmental Information Regulations**

Records will be managed in accordance with these regulations and the associated code of practice.

6. Records Identification Requirements

The identification of records will follow best practice in records management and allow for users of the records to identify and track particular records. The Council's identification systems require:

- classifying of records into series that have meaningful titles and/or a consistent reference code;
- making those individuals responsible for creating records, responsible for allocating them to a series and, if necessary, a sub-series;
- having sequences of reference numbers that can cover series containing either, or both, electronic and paper records;
- checking that the correct records have been allocated to the sequence and that meaningful titles are used;
- auditing lists of the references used so that the identification system makes sense and records can be found in appropriate search sequences.

7. Preservation Requirements

(a) A preservation requirement aims to minimise the risks associated with technological changes and ensures that records remain intact. It also allows for any non-technical changes, for example always having an associated context, which remains comprehensible as the organisational structure changes.

(b) The Council will therefore seek to preserve electronic records during any change in infrastructure. Preservation needs will be satisfied when there are changes in:

- the technology that processes the electronic records and how this affects the way records are processed throughout the record's existence;
- organisational structures and how these are interpreted and give the records context;
- the definition of terms used in the metadata and within the records themselves;
- the classification of the electronic records, including how the records are grouped and described, so that they can be presented in a way consistent with the original understanding of the subject when the record was created.

8. Policy Review

Departments will adhere to this RM Policy in the operation of their records management activities. Internal Audit may undertake periodic planned audits to assess how this RM Policy is being put into practice. The audits will seek to highlight where non-conformance is occurring and suggest a tightening of controls and adjustment to related procedures.