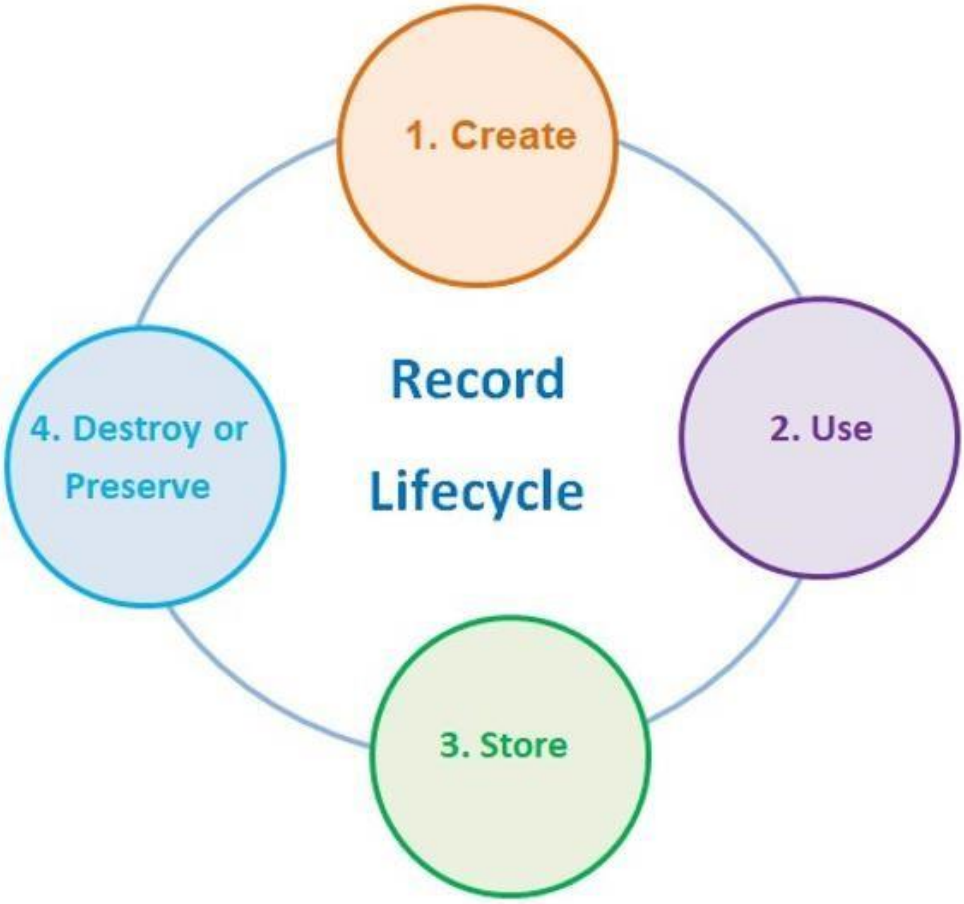
Record Management Policy



Document Control

Owner	Data Protection Officer
Author	Complaints and Information Requests Manager
Last Reviewer	Head of Assurance
Approver	Audit Panel
Date of Approval	June 2024
Date of Next Review	2026
Version	2.0
Classification	Public

Version Number	Date	Changes	Approved by
1.0	July 2021	Original document	Audit Panel
2.0	May 2024	Refreshed Document	Audit Panel

This is a live document effective from the issue date. It supersedes any previous version of this document, which are now withdrawn.

Further information, advice or guidance about this document can be obtained from:
The Information and Data Team
informationanddata@tameside.gov.uk

1. INTRODUCTION

The public has a right to access information held by or on behalf of the Council (a public authority) under the Freedom of Information Act 2000 and Environmental Information Regulations 2004. Additionally, individuals also have rights to access their personal data under the General Data Protection Regulations (UK GDPR) and Data Protection Act 2018. These rights are diminished if information cannot be found when requested or, when found, cannot be relied upon as authoritative.

Good Records Management will benefit all staff and Service Areas in the Council. Benefits include but are not limited to:

- A reduction in time spent searching for information;
- Improved information integrity due to fewer versions and duplications of documents;
- Improved transparency and accountability;
- A reduction in storage costs as data is cleansed;
- Improved access to information;
- An open and transparent foundation for decision-making;
- Preservation of the Council's corporate memory;
- Supported continuity in the event of a disaster;
- Enhanced customer service and improved reputation with partner organisations;
- Protection and support in litigation;
- Compliance with legislation and regulations such as the UK GDPR, DPA 2018, employment legislation and health and safety legislation;
- Improved ability to demonstrate corporate responsibilities;
- Business intelligence and analysis of data are reliant on excellent record keeping;
- Records of value to Tameside are identified and held by the Archive.

Poor Records Management creates risks for the Council such as:

- Staff time wasted searching for information;
- Inconsistent or poor levels of service;
- Poor decisions based on inaccurate or incomplete information;
- Financial or legal loss if the information required as evidence is not available or cannot be relied upon;
- Non-compliance with statutory or other regulatory requirements;
- Failure to handle confidential information with an appropriate level of security;
- Unauthorised access to confidential records and information, breaching UK GDPR regulations;
- Failure to protect information that is vital to the continued functioning of the Council
- Inadequate business continuity planning;
- Staff time wasted considering issues that have previously been addressed and resolved;
- Unnecessary costs caused by storing records longer than they are needed;
- Unauthorised disposal of records and information;
- Loss of reputation as a result of all the above, with damaging effects on public trust.

2. SCOPE AND DEFINITIONS

This policy sets out recommended good practices for the management of all records, paper and electronic, including those in dedicated line of Business Systems.

TERM	DEFINITION
Record	Information, in any format, created or received by the Council to support and provide evidence of activities and business transactions. This may include, but is not limited to, personal data.
Retention and disposal schedule	A document detailing how long records need to be retained before they can be destroyed.
Information Asset Register (IAR)	A document that records the assets, systems and applications used for processing or storing data across the organisation. There are elements of overlap between IAR ROPA and retention and disposal schedules
Record of Processing Activity (ROPA)	A document, required by Art.30 UK GDPR, which records all data processing activities under a Data Controller's (and where applicable, their representative) control. Art.30 sets out a prescribed list of the minimum detail required. There are elements of overlap between ROPA, IAR and retention and disposal schedules
Personal data	Information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council are legally responsible for the storage, protection and use of all personal information held as governed by the UK GDPR and DPA 2018.

3. SUMMARY OF RECOMMENDED GOOD PRACTICE

Good practice in records management is made of a number of key elements. Guidance on each element is given in this policy.

- Service areas clearly outline the roles, responsibilities and expectations of Records Management;
- Service areas only keep the records they need for business, regulatory, legal and accountability purposes;
- Service areas keep their records in systems that enable records to be retrieved as necessary; Service Areas know what records they hold and where they are, and should ensure that those records remain usable for as long as they are required;
- Service Areas store records securely and control access;
- Service Areas know how long they need to keep particular records, appropriately dispose of records when they are no longer needed and be able to explain why records are no longer held;
- The Council ensure that records shared with other bodies or held on their behalf by other bodies are managed in accordance with this policy.

4. ROLES, RESPONSIBILITIES AND EXPECTATIONS OF RECORDS MANAGEMENT

Records Management is a core corporate function. Consideration of records management is needed when planning or implementing ICT systems, extending staff access to new technologies and during re-structuring or major organisation changes.

ROLE	EXPECTATIONS
All employees, Elected members and those individuals engaged by the Council	To manage information and create records in line with the Council's policy and procedures. All staff and individuals engaged by the Council should ensure that they are familiar with and follow any management procedures in their service.
Team Manager	To manage information and create records in line with the Council's policy and procedures. All staff and individuals engaged by the Council should ensure that they are familiar with and follow any management procedures in their service.
Senior Management Team	It is the responsibility of individual service areas to carry out and review the necessary retention and disposal requirements for their records, with advice and support from the Records Manager. The Chief Executive has senior management responsibility for records management within the Council.
Records Manager	The Records Manager has day-to-day oversight of records management within the Council. The Records Manager will: • Develop policies and procedures that ensure that service areas have the ability to be compliant with policy and legislation. • Provide regular training programmes for Council staff and those individuals engaged by the Council. • Develop guidance and advise colleagues across the Council on records management issues. • Provide advice on adequate storage for records and subsequent monitoring of such areas.

All Council staff will be made aware of their responsibilities and supported through regular training programmes and guidance.

5. WHAT RECORDS NEED TO BE KEPT

Service areas need to consider what records they are likely to need, and the risks of not having those records, taking into account the following factors:

- The legislative and regulatory environment within which they operate. This will be a mixture of generally applicable legislation and specific legislation applying to the service;
- The need to refer to authoritative information about past actions and decisions for current business purposes;

- The need to protect the legal and other rights of the Council, staff, and stakeholders.
- The need to explain, and if necessary justify, past actions in the event of an audit, public inquiry or other investigation.

All staff will be aware of which records the Council decide to retain through the Retention and Disposal Schedule, as well as where those information assets are stored through the IAR.

All staff have a responsibility to keep accurate and complete records and are aware of the need to give those records titles that reflect their specific nature and contents to facilitate retrieval.

Ephemeral material can be disposed of on a routine basis, for example, printouts of electronic documents, trivial emails, and personal copies of documents.

6. DIGITAL RECORD SYSTEMS

The Council hold records on a number of different systems to meet the service area's specific needs. All record systems should have the following characteristics:

- Be easy to understand and use to reduce the effort required of those who create and use the records within them;
- Enable quick and easy retrieval of information. This should include the capacity to search for information requested under the Freedom of Information Act 2000 or Environmental Information Regulations 2004, or Individual Rights covered by UK GDPR and the Data Protection Act 2018;
- Enable routine records management processes to take place. Systems should be able to delete specified information and leave the rest intact;
- Enable the context of each record, and its relationship to other records, to be understood;
- Protect records from accidental or unauthorised alteration, copying, movement or deletion;
- Provide secure storage for the level of protection required by the nature, content and value of the information in them;
- Enable an audit trail to be produced of occasions on which selected records have been seen, used, amended, and deleted.

Records in digital systems will not remain usable unless precautions are taken. Corporate line of business systems and shared files must be used to store all electronic records and information. ICT have strategies for continued maintenance and backup processes to ensure that information within these systems and shared drives remain intact, reliable and usable. Any information stored outside of the line of business systems and shared drives is not maintained by ICT and is therefore vulnerable. Under no circumstances should any operational/service data (including personal and non-personal data) be stored on an employee's laptop hard drive as that record cannot be backed up or retrieved by ICT in the event of a laptop failure.

7. SCANNING RECORDS

An electronic record, scanned from the original paper record, will be accepted by a court or other legal body as long as it can be proven that it is a true copy. A clear scanning procedure will demonstrate beyond reasonable doubt that the original document has been scanned in its entirety.

All MFDs have the ability to scan and send the record to your email address or shared file. ICT Services can advise on specific scanning requirements such as adding workflow to records or scanning directly into a line of business systems by contacting ict.training@tameside.gov.uk.

Once scanned, the paper copy can be destroyed to safeguard against duplications, ensuring that personal information is confidentially destroyed.

Important Records such as deeds, contracts, guarantees or certificates, should not be destroyed without advice from Legal Services and the express permission of those involved in the contract.

8. PHYSICAL STORAGE

The effectiveness of records storage depends on knowledge of what records are held, what information they contain, in what format they are accessible, what value they have to the service area and how they relate to business functions. Without this service areas will find it difficult to:

- Locate and retrieve information required for business purposes;
- Locate and retrieve information required to respond to an information request;
- Gather and maintain data required on the IAR and ROPA;
- Effectively manage the risks associated with storing records (both paper and electronic);
- Ensure records are disposed of when no longer required.

Wherever possible, paper documents should be scanned and retained in an electronic format to keep the information in a readable condition and to reduce the inconvenience and cost of physical storage.

Storage for non-electronic records needs to be well organised, with all files labelled, numbered, and indexed accurately. Services need to be aware of any specific requirements for records storage that apply to them.

Storage facilities need to be suitable to preserve records and protect them from damage, theft and disaster (i.e. fire, water). Consideration needs to be made in regard to the future risks for non-electronic records to ensure that they remain reliable and usable for as long as required. Risks to consider include:

- The delicate nature of ageing paper, including carbon paper;
- The fading of pictures, photocopies and handwritten text;
- Records are stored on defunct technology, such as cassettes, microfiche, and disks.

The whereabouts of records should be known at all times and movement of records between storage areas and office areas should be logged.

9. RECORDS SHARED WITH AND STORED BY EXTERNAL BODIES

When working in partnership with other organisations, sharing information and contributing to a joint records system, services should ensure that all parties agree to protocols that specify:

- What information should be kept, and by whom;
- What level of information security should be applied;
- Who should have access to the records;
- What disposal arrangements should be in place;
- Which organisation is responsible for responding to information requests?

Particular protection should be given to confidential or personal information. Protocols should specify when, and under what conditions, information and records will be shared and details should be kept of when this information has been shared.

The Council are responsible for ensuring that contractors and other organisations creating records on behalf of the Council are storing and maintaining records to the standard set out in this policy. This can be done through Data Processing and Sharing Agreements, please contact to the Information Governance team (information.governance@tameside.gov.uk) for more information.

10. RETENTION AND DESTRUCTION

It is important that records are retained only for as long as needed to serve their business function and/or comply with legislation. The untimely disposal of documents will cause the Council:
Difficulty in defending litigious claims;

- Operational problems;
- Failure to comply with Freedom of Information Requests or Environmental Information Regulations requests;
- Failure to comply with Subject Access Requests;
- Breach of data protection legislation if data is retained for longer than it should be.

Reference should be made to the Retention and Disposal Policy.

11. LEGISLATION AND RELATED POLICIES

This Policy has been written with reference to the **Code of Practice on the Management of Records (issued under Section 46 of the Freedom of Information Act 2000).**

12. SUPPORTING POLICIES

This policy should be read in conjunction with the Information Governance Framework, and in particular the following policies and procedures:

- IT Security Policy;
- Data Protection Policy ;
- Scanned Documents;
- Paper Records Secure Handling and Transit;
- Records Retention and Destruction Policy

13. POLICY REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years or when there are changes to legislation.

Appendix 1 - TIPS FOR EFFECTIVE RECORDS MANAGEMENT

Creation

Records should be created at the time of, or as soon as practicable after the event to ensure they are accurate and reliable.

Think about how you name your records and agree a format within your team or line of business system. This will make it easier to identify and retrieve documents. Top tips include:

- Keep file names short, but meaningful;
- When including a number in a file name always give it as a two-digit number, i.e. 0199, unless it is a year or another number with more than two digits;
- If using a date in the file name always state the date first and 'back to front'. Use
- YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY;
- When including a personal name in a file name give the family name first followed by the initials;
- Order the elements in a file name in the most appropriate way to retrieve the record;
- The file names of records relating to recurring events should include the date and a description of the event;
- The file names of correspondence should include the name of the correspondent, an indication of the subject, the date of the correspondence and whether it is incoming or outgoing correspondence;
- Avoid using repetitive words such as 'draft' or 'letter' at the start of file names;
- The version number of a record should be indicated in its file name by the inclusion of 'V' followed by the version number;
- Avoid using non-alphanumeric characters in file names, for example " £ $ % ^ & * ()!;
- Line of business systems often have standardised formats for file storage, contact ICT for more information.

Use

Agree on a procedure within your teams as to where electronic and paper records are stored. Ensure all documents are filed in the electronic shared drive and not on individual desktops.

Assign responsibility for maintaining shared files to a job role or member of the team.

Avoid creating duplicate or unnecessary records. Rather than email attachments to your team, save the document in your shared drive and email a hyperlink to the team.

Avoid storing duplicate drafts of the same record. Ensure that old drafts and duplicate versions are deleted to avoid unnecessary confusion.

Discuss records management in team meetings.

Email Management

Be aware that anything you write in an email could be subject to release under FOIA/SAR. Always consider the content and tone of your emails before you send them.

Delete any emails which you do not need to retain. These will include emails sent for information only, e.g. most CC emails since you are not the main recipient, outdated information or personal emails.

Check emails before you archive to ensure that you are only saving the information you need. The retention period for all emails is 2 years. It is important to ensure any emails to be stored for retention reasons are saved in line of business or shared files accordingly.

Store

Wherever possible, scan paper records and keep them electronically.

Distribute documents electronically before meetings rather than taking printouts with you, either by email or via shared drives. This will reduce the storage of duplicated documents. For democratic and executive meetings meeting papers are electronic through the use of modern.gov software.

End of Retention Reviews: Destroy or Preserve

Hold record clean-up days on a regular basis.

During the review consider:

- Do you need the information to carry out your business?
- Is there a legal requirement to keep the information?
- Do you need the information for financial purposes?
- Will you need the information to explain why you arrived at a particular decision?
- Will you need the information if your decision is challenged in court?
- Will you need the information to be publicly accountable for your policies and decisions?
- Will you need the information to help with similar situations in the future?
- Will you need the information to defend your rights and responsibilities, or the rights and responsibilities of others?
- Does the information have value for historical research purposes?