Records Management Policy

Live from:	April 2025
Live until:	March 2028
Contact:	records@middlesbrough.gov.uk

Title	Records Management Policy			
Creator	Author(s)	Paul Jemwa (Records Manager)		
	Approved by	Ann-Marie Johnstone (Head of Governance, Policy and Information)		
	Department	Governance, Policy and Information		
	Service area	Legal and Governance Services		
	Head of Service	Ann-Marie Johnstone		
	Director	Charlotte Benjamin		
Date	Created	2025/04/30		
	Submitted	2025/04/30		
	Approved	2025/xx/xx		
	Updating Frequency	3 years		
Status	Version: 3.0			
Contributor(s)	Interim Head of Governance, Policy and Information (SIRO); Governance and Information Manager; Data Protection Officer;			
Subject	Records Management			
Type	Policy			
	Vital Record		EIR	
Coverage	Middlesbrough Council			
Language	English			

Document Control

Version	Date	Revision History	Reviser
0.1	20181005	First draft	L Hamer
0.2	20190204	First revision	AM Johnstone
1.0	20190529	Finalised	P Stephens
2.0	20220503	Update	L Hamer
3.0	20250xxx	Review	P Jemwa

Distribution List

Version	Date	Name/Service area	Action
1.0			
2.0	20220504	Intranet	Published
3.0	20250xxx	Intranet	Published

Summary

This policy is part of the framework underpinning the Council's Information Strategy and is aligned with the statutory Code of Practice on the management of records and sits within the Council's Information Governance Policy Framework.

It sets out how the Council will manage its records, in line with the vison of the strategy that '**the right information will be available to the right users, at any time, accessible and used ethically to support achievement of the Council Plan Ambitions'.**

Managing Records effectively will support delivery of the Council's emerging Digital Strategy.

The following sections outline:

- the purpose of this policy;
- definitions;
- scope;
- the legislative and regulatory framework;
- roles and responsibilities;
- supporting policies, procedures and standards; and
- monitoring and review arrangements.

Purpose

The increasing reliance on electronic records, with more information being created and received digitally, has added a new dimension to the challenges that Middlesborough Council faces. The growth of digital technology has provided different ways for us to communicate and share information which makes information and records management even more complex. A solution to transforming ways of working with, storing digital information, providing structure and consistency across dedicated corporate storage platforms is SharePoint Online.

Through the implementation of this policy the Council aims to:

1. Provide guidance to teams across the organization to cleanse their existing content, removing redundant, obsolete and trivial information so that only valuable content is migrated to SharePoint Online.

2. Rationalise and map content held on existing platforms to new locations in SharePoint Online, identifying library column/metadata requirements, site structures, access permissions and retention assessment.

4. Provision of information management advice and guidance to Information Owners and end users on the current and future structure and organization of their documents, use of metadata and other SharePoint functionality, customizing new sites and libraries and configuring site features appropriately.

5. Analysis of discovery phase results to understand individual team requirements for their information management needs, finding and recommending solutions (administrative and technical) to any complex operational issues or requirements,

6. Supporting the governance of electronic records management solutions through maintaining high quality documentation and managing business input into decisions on change priorities

7. Digitise, archive or store historic records as appropriate

This will deliver the following benefits:

- the Council will ensure that, where and when required, authoritative information about its past activities can be found and used for current business (corporate memory);
- the Council will be able to demonstrate compliance with its legal duties, and respond to public information requests more efficiently;
- the Council will become more transparent, proactively and routinely publishing data of public interest; and
- the Council will achieve a more effective use of resources, through the ongoing digitisation of records and the correct implementation of the corporate Records Retention Schedule.

Effective records management will also help the Council mitigate the following risks:

- loss of records vital to effective operations;
- taking poor decisions based on inadequate or incomplete records;
- failure to handle personal or confidential information with the required level of security;
- criticisms or sanctions from the Information Commissioner for non-compliance; and
- financial losses due to the lack of reliable evidence, or incurring unnecessary costs for date storage.

Definitions

Topic	Definition
Records	Records are defined as information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. Information that is only of short-term value, and contains little or no ongoing administrative, financial, legal, evidential or historical value is not considered a record. If well-kept, records tell us what happened, what was decided, and how to do things. They are used as the basis on which decisions are made, services provided, and policies developed and communicated. Records can be in either physical or digital format.
Records Management	Records management is the regime an organisation puts in place to manage records through the lifecycle of creation, receipt, maintenance, use and destruction. It ensures that a record has:

	• Authenticity– it is what it says it is; • Reliability – it can be trusted as full and accurate; • Integrity – it has not been altered since it was created or filed; and • Usability – it can be retrieved, read and used.
Sensitivity Labels and Information Security Classification	The Council utilises the UK Government's security classifications to help it identify, protect and work with information of different sensitivities. As the Council does not access SECRET or TOP SECRET information, all of its information will fall under the Government's OFFICIAL classification. The OFFICIAL classification is broad and includes information that is sensitive and must not be shared freely, including personal data that must be protected under data protection legislation. Applying sensitivity labels to content such as documents and email ensures that we keep our information secure by stating how sensitive certain information is.
Records retention and disposal	This schedule provides guidance on how long records created and held by the Council should be retained for along with the legislation that governs that decision to ensure we maintain compliance.
Records access	Enabling access to records is a legal requirement under Data Protection Law individuals who have information stored in relation to them have the right to request access to that information under Subject Access via a Subject Access Request. Individuals can request detail about the information held on them, how it is being used, who it is being shared with and where the information was obtained from.
Records security	Records must be held securely in order to maintain their integrity and security. Paper records should be secured by way of access and physically held appropriately, electronic records should be protected by necessary and appropriate technical security controls to strengthen protection against unwanted access.
Historical records	Are held in order to maintain their protection and preservation for the future. There are a number of records which hold extensive retention periods and these must be retained, as well as records which hold significant historical value to the organisation.
Records archive	Records held securely to maintain preservation by Teesside Archive who collect, catalogue and preserve historical documents relating to Middlesbrough, Stockton, Hartlepool and Redcar & Cleveland and make them available for the public.

Information Asset Registers	Information Assets Registers records assets, systems and applications used for processing or storing personal data across our organisation and records ownership and responsibility to individuals for the security and maintenance for that information.

Scope

This policy applies to all employees (both permanent and temporary), contractors and consultants of the Council who are given the authority to create records or to access them.

It applies to all records owned by the Council, whether they are created or received and managed directly, or by third parties on its behalf. It also applies to records created, received or managed by the Council in partnership with, or on behalf of, other organisations.

Legislative and regulatory framework

Key elements of the legislative and regulatory framework for records management are set out below. Failure to comply with this framework can lead to significant financial penalties, criminal prosecution and non-criminal enforcement action.

Records management does not exist in isolation, and connects to other information governance disciplines, such as data protection, and corporate governance arrangements including risk management.

EU General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018	The DPA places a duty on the Council to manage personal data in a way that is lawful and fair, not excessive, secure and proportionate (e.g. not to retain it longer than required). It also obliges the Council to respond to requests from personal data from the data subject.
Digital Economy Act 2017	Provides government powers to share personal information across organisational boundaries to improve public services.
Freedom of Information Act (FOIA) 2000	Under the FOIA, the Council has a duty to make information available to the public upon request, unless specific exemption(s) apply. It is also obliged to proactively and routinely publish information that has been frequently requested in the past in its Publication Scheme.
Local Government Acts 1972, 1985, 1988 and 1992	Establishes requirements to manage records and information and gives implied authority to share certain kinds of information with partners.
Code of Practice on the management of records issued under section 46 of the FOI Act 2000	Issued under s.46 of the FOIA, the code sets out good practice in records management and set out how public records (as defined by the two Public Records Acts) will be transferred to places of deposit.

Other Regulations and Codes of Practice	Records management practice is also informed by range of other regulations and codes of practice, including: • Privacy and Electronic Communications Regulations 2003 (PECR); • Environmental Information Regulations 2004 (EIR); • Re-use of Public Sector Information Regulations 2005; • 'Caldicott principles' on NHS patient information (revised 2013) and the NHS Data and Protection Toolkit; and • ISO 15489 Records Management.

Roles and responsibilities

Effective records management is the collective responsibility of all those individuals named within the scope of this policy.

Senior Information Risk Owner (SIRO)	Responsible for the overall management of information risk within the Council, advising the Chief Executive, management team and Information Asset Owners, and ensuring that staff training is available and fit-for-purpose. The role is undertaken by the Head of Governance, Policy and Information, who is also responsible for the Information Strategy.

Records Manager	Responsible for the development and implementation of this policy and supporting procedures, providing advice and checking compliance to ensure the Council's records are well-kept and that the systems used to hold them are fit-for-purpose and in line with the statutory Code of Practice. The Records Manager is responsible for records held by the Council including inactive records where an information asset owner cannot be identified. This policy provides a clear mandate for the Records Manager to act in this key role.
Analytics and Data Manager	Responsible for the development and implementation of the Council's Data Management policy and supporting procedures, to ensure that the Council meets its obligations in respect of data integrity, statutory returns to the Government and data transparency.
Public Information and Information Requests Team	Responsible for provision of advice and guidance to the Council on its obligations in relation to statutory public information requests (including Freedom Of Information and Environmental Information Requests) and monitoring compliance with these.
Data Protection Officer	Responsible for provision of advice and guidance to the Council on its obligations in relation to data protection.
Complaints and Subject Access Team	Responsible for handling and resolving complaints received and fulfilling Subject Access Requests. The team provides support to staff responding to complaints and ensures that statutory timescales are adhered to for responses for both complaints and Subject Access Requests. The team will monitor and identify trends which can be used to improve services.
Information Asset Owners (Heads of Service)	Responsible for maintaining comprehensive and accurate information asset registers (IARs) for their service areas, and ensuring that: • staff in their service area are aware of their responsibilities and appropriately trained; • records are managed in line with this policy and its supporting procedures; • where possible, all data is created and held within a digital format; • those paper records that are held are managed properly; • access to and sharing of records is appropriate; • records are retained, archived and destroyed in line with the Council's

	Retention Schedule, and ICT systems enable this; and • identifying and escalating information risks to the SIRO.
All managers	Responsible for overseeing day-to-day compliance with this policy by their staff and other personnel they manage.
All staff, contractors, consultants, interns and any other interim or third parties	Responsible for creating, accessing, using and managing records and record keeping systems in accordance with this policy and its supporting procedures. Capturing records and required metadata into specified record keeping system(s). Responsible for identifying records at risk of damage to the Records Manager.
Information Strategy Group	Operational group of key officers led by the SIRO responsible for implementing the Information Strategy, in conjunction with Information Asset Owners.
Risk Management Group	Cross departmental group of senior officers responsible for ensuring the Council has in place a suitable risk management framework. The group has reporting lines to enable risks in relation to record management and other information issues to be escalated by the SIRO and considered as necessary.

Supporting policies, procedures and standards

The following policies, procedures and standards will be implemented across the Council to ensure that the Council's records are managed effectively and securely.

Data Management Policy	This provides a framework for effectively standardising, managing, linking and exploiting data throughout its lifecycle, and to ensure that the Council meets its obligations in respect of data integrity, statutory returns to the Government and data transparency.
Data Protection Policy	This ensures that the Council continues to treat personal data safely, securely and ethically; deals with incidents swiftly and learns lessons from them; and is fully compliant with the DPA.
365 Email Policy and Procedure	This sets out business rules and requirements for the use of email, in particular how these should be stored when considered a record to be retained.
SharePoint Procedures	These sets out business rules in respect of the use of SharePoint as the proper tool for the storage and referencing of digital records.
Public Information and Information Requests Policy and Procedures	This establishes the corporate framework for responding to statutory information requests, and to proactively identify information to be routinely published.

Print and Mail Procedure	This sets out business rules designed to minimise printing and mail within the Council.
Records Retention Schedule	This defines how long different records should be retained to comply with legal, regulatory or other requirements e.g. required to be retained for historic significance, statistical interest or other reason as defined by the statutory code of practice or another legal basis. Schedule sets out the proper arrangements for archiving and destruction.
Destruction Certificate	Record of the legal basis and process followed for the destruction of records. Completed forms once authorised by the Manager and or Records Manager should be retained in service for audit purposes.
Surveillance Policy	This ensures that the Council's legal covert surveillance powers are well-understood by employees, and their use remains necessary, proportionate and justified, and is kept to a minimum.
Scanning Procedure	This sets out business rules and requirements for the appropriate digitisation of physical records, to reduce storage requirements, increase accessibility and improve compliance with the Records Retention Schedule. As included in Appendix A.
Secure Working Policy	This sets our rules around access rights and enhancing cyber security, within the context of agile working.
Vital Records Standards	This sets out how vital records will be identified and the steps to be taken to ensure their protection and preservation.
Business Continuity Plans	These identify those vital records required to support delivery of critical services.
Disaster Recovery Plan	This identifies priorities and recovery timescales for access to ICT systems and digital records in the context of business continuity.

Monitoring and review arrangements

The implementation and effectiveness of this policy and its supporting procedures will be reviewed on a quarterly basis by Information Strategy Group, using the following metrics:

- print and mail volumes;
- data breaches due to poor records management practice;
- proportion of corporate records that are digital; and
- proportion of digital records that are held in SharePoint Online.

The SIRO will provide a quarterly update to the Council's Risk Management Group on overall information risk, and an annual report to management team and Audit Committee.

This policy will be reviewed every three years, unless there is significant development that would require a more urgent review e.g. new legislation.

Appendix A

Scanning Procedure Notice

This document is controlled and maintained according to the documentation standards and procedures as detailed and included within the Information Strategy Framework. All requests for changes to this document should be sent to the author(s).

1.0 Purpose

The purpose of this policy is to identify common standards and practice in relation to the conversion of analogue records to digital (electronic) format.

2.0 Scope

This policy covers the conversion of any Middlesbrough Council documents or records into digital format.

3.0 Background

There are many business reasons why digitisation projects may be undertaken within Middlesbrough Council and the use of this type of technology can bring clear business benefits:

- capacity to access the images concurrently
- access from multiple locations
- incorporation into other systems
- application of consistent approach to naming and indexing
- provision of secure master image
- reduction in storage of paper records

However, conversely there are increased risks associated with digitisation:

- obsolescence of technical standards
- additional costs to maintain digital image environment
- legal admissibility

4.0 Vision

Over time the Council has moved to a greater reliance on the use of electronic documents and records as opposed to paper based records. This has resulted in an improved access to information, increased ability to store information when appropriate and more robust security. Although a ‘paperless office’ may not be achievable in our current context we will work towards holding the master copy of records and documents in digital format. This means we will need to employ increased use of scanning for based paper documents and for incoming external paper documents.
We will continue to manage all documents and records within our current legal and regulatory framework and Council policies.

5.0 Project Initiation

All digitisation projects should follow the Council project route and will require a mandate and project initiation document to identify scope, business benefits, cost and technical standards employed in the project. Quality assurance and ongoing management will be implemented.

6.0 Options for Methodology

In-House – the digital images / paper documents are delivered from within the Council either by a specific task group created for the purpose or by individuals as part of their daily activity.

Out-sourced – the work is allocated to an external agency through the Council procurement process.

Quality assurance processes must be established and documented to ensure that the project meets expected outcomes.
The approach should be regularly reviewed where projects are over an extended period of time.

7.0 Technical Standards

Software: There are many options for scanning software which perform the digital conversion from paper to digital image. Any software employed in-house needs to meet the Councils technical requirements.
However, it is the output of the digital image that is important in terms of standardisation.

Hardware: In a similar way the restrictions on hardware are related to the general requirements and standards for the use of peripheral equipment on the council system. There are a number of issues to consider when addressing technical standards (Appendix A contains a technical specification)

File Format:

- Technical specification needs to be available
- Format should be supported by standard software and operating systems used within Middlesbrough Council
- Formats should be compatible with viewing players used by Middlesbrough Council
- File formats encode information into a form which can be rendered comprehensible by software. File formats are vulnerable to change in rapidly evolving technical environments. Consideration should not simply be given to immediate requirements but also longer-term considerations i.e. if a scanned image needs to be retained for 75 years what are the implications of selecting a particular file format. The National Archive recommends considering the following when selecting a file format, open standards, ubiquity, stability, interoperability and viability.

Resolution

Resolution needs to be of sufficient quality to meet the required uses of the scanned document, this will vary in accordance with use and end user consultation is an important aspect of the decision.

Compression

Where compression techniques are applied consideration must be given to whether any data loss can occur because of the compression and if this has any bearing on the legality of the record. This will depend on the function or intended use of the document and the area of activity to which it relates. If there is any uncertainty, advice should be sought from Records Management.

Colour Management
Consideration needs to be given to how good the image needs to be for the required use of the document.

8.0 Preparation of documents to be digitised

- An assessment of the robustness of documents to be digitised is required. Quality of paper and age will be a consideration of scanning quality.

- Physical preparation of documents such as batching or removing staples etc. should be estimated as part of the overall costs / time consumption (if in house) of the project.

- Indexing. The index data for an image will need to be input into the corporate records management system (SharePoint Online) Care should be taken that appropriate indexing information is recorded to link the image and its filename.

9.0 Metadata

Metadata, or data about the context and creation of the document, is an important aspect of maintaining any records but this is even truer of scanned images. It is important that information that will be used to make decision about managing, accessing and ultimately disposing of the documents in the future. It is important to remember that if the correct metadata is not captured with the document at the point of scanning then it is highly unlikely that it will be associated with the image and become irretrievable
.
There are two principal types of metadata that are required to be captured with digitised images:

i) metadata about the image and the process that created it e.g. image identified, date of digitisation, name of creator.

ii) Metadata about the content

Accessibility; addressee; audience; contributor; creator; date; description; disposal; format identifier; language; location; preservation; publisher; rights; source; status; subject; title; type.

10.0 Legal Admissibility

Many documents and records used by Middlesbrough Council can potentially be required in support of litigation and submitted as evidence as part of legal or tribunal proceedings.

Scanned images produced from these images are normally accepted by courts as evidence. However to ensure that the correct 'weight of evidence' is attributed to these documents it is important that extra measures are applied to conversion of documents that have a high probability of being challenged in litigation.

An appraisal of the likelihood of documents being needed for evidence should be completed. If the conclusion is that there is a high potential for any document to be challenged in court proceedings then guidance as laid out in BIP 0008, the '*Code of Practice for Legal Admissibility of Information stored on Electronic Document Management Systems'* should be consulted. 'The criteria for establishing this high potential should be based upon the frequency that we regularly submit the documents in litigation and our knowledge of the frequency of challenge, based on case law.
Advice can be sought from Records Manager.

11.0 Retention of Documents

There are two principal reasons for retaining paper documents after they have been scanned:

1. the scanning has taken place for reasons of accessibility and speed of processing but there is a legal or regulatory requirement to retain the original document. Details on retention are also in the corporate Retention and Destruction guidance.

2. Originals are retained on a short term basis to ensure that the validity and quality of the scanning process has met expected requirements. This should not be an indefinite arrangement.

On destruction of the original paper documents the scanned image becomes the master copy. All destructions of confidential paper documents should take place through the Council Office Recycling Confidential Waste Services.

Appendix B

Document Type	Resolution	Bit Depth	File Format	Compression?
Text Only Monochrome	>300 dpi	1 bit (bit-tonal)	TIFF PDF/A JPEG 2000	
Documents with water-wash or grey text	>600 dpi	8 bit greyscale	TIFF JPEG 2000 PDF/A	
Colour documents	>600 dpi	8 bit colour (minimum)	TIFF JPEG 2000 PDF/A	
Monochrome photographs	Sufficient to provide >3000 pixels across long dimension	8 bit grey scale	TIFF JPEG 2000 PDF/A	
Colour photographs	Sufficient to provide >3000 pixels across long dimension	24 bit colour	TIFF JPEG 2000 PDF/A	

The table above provides a minimum expected standard for scanned documentation. Variation for the defined standard need to be approved.