

Records Management Policy



North
Tyneside
Council

Contents

1. Objective.....	2
2. Purpose.....	2
3. Scope.....	2
4. Roles and responsibilities.....	3
5. Record retention and disposal.....	3
5.1 What records should we keep?.....	4
5.2 Do we need to keep every version?.....	4
5.3 Where should we store records?.....	4
5.4 Email.....	4
6. Suspending disposal of records.....	5
6.1 Suspensions.....	5
7. Training and awareness	5
Document Control.....	5

1. Objective

The objective of this policy is to define a framework for North Tyneside Council ('the Authority') to manage data, information and records in compliance with its statutory obligations. This policy contains overarching requirements to ensure that the Authority:

- creates and manages accurate, authentic, reliable and accessible data, information and records to meet the authority's business needs
- identifies data, information and records which should be disposed of and disposes of it in line with the Authority's information security requirements
- includes all business-critical data, information and records in business continuity plans
- can identify information which could be published as part of the Open Data and Transparency programme.

2. Purpose

The Authority creates, uses, and receives records which are a valuable resource and an important asset, supporting its legal, financial, business and administrative requirements. The systematic management of the Authority's records, from creation to disposal, is essential to protect and preserve them as evidence of actions, to support present and future activities and business decisions, and to ensure accountability to present and future stakeholders.

The Records Management Policy sets out the Authority's commitment to consistently and securely create, keep, and dispose of high-quality records documenting its business and activities. It sets out the principles of good records management which shape the development of operational procedures. The policy also defines the characteristics of high-quality records, and describes the mechanisms of planning, governance and training that support compliance with the policy.

3. Scope

The Authority is committed to creating, keeping and managing data, information and records which document its principal activities.

This policy covers data, information and records regardless of the media in which it is stored (i.e. physical or digital formats - including e-mails) which are deemed to be part of the corporate record. This policy covers all data, information and records created by the Authority including those created by contractors and partners working on the Authority's behalf regardless of where they are created, stored or managed.

Records held by schools are the responsibility of the individual school and are outside of the scope of this policy. In the event of a school closing, the Authority becomes responsible.

4. Roles and responsibilities

All Authority employees are responsible for creating and maintaining data, information and records in relation to their work that are authentic and reliable.

The Information Governance and Compliance Manager is the Data Protection Officer. The Information Governance Team will be responsible for providing advice, policies, protocols and procedures to assist service areas to achieve compliance with all Information Governance legislation, data, information and records management practices.

The Director of Resources is the Senior Information Risk Owner (SIRO). The SIRO is responsible for ensuring that the appropriate resources are available to implement and monitor the Records Management Policy.

Each Director is the Information Asset Owner (IAO) for their directorate. The IAO's role is to understand what information is held within their directorate, how it is used, who has access and why, so that they can understand and address risks to the information.

5. Record retention and disposal

All data, information and records (regardless of the media or format in which they are stored) must be retained for the period identified in the corporate retention schedule. The retention periods listed in the schedule are the minimum length of time which the data, information and records must be retained. Where necessary data, information and records may be retained for longer periods of time.

The Corporate Retention Schedule has been created to support the Authority to meet its statutory obligations to ensure that information is retained for the correct period and then disposed of appropriately.

It is unlawful to retain personal information for longer than necessary. If any delay is anticipated then this should be raised with the Data Protection Officer with a timescale for when the information will be disposed of.

The Corporate Retention Schedule sets out how long information should be retained before it is disposed of or, where it is deemed to be of permanent historical value, transferred to the Local History/Archives Service.

Staff should seek guidance from line managers in departments, or the Data Protection Officer, if they feel that any changes to the schedule(s) are required.

The Corporate Retention Schedule applies to any media or format that recorded information may come in, digital or physical. Information that has reached the end of its retention period should be disposed of or transferred where appropriate.

Documents that are not covered by the Corporate Retention Schedule need to be destroyed as soon as they become obsolete.

5.1 What records should we keep?

Any information concerning the core business of the Authority, or that has a continuing value, should be retained as a record.

Information with a short life span or that is a duplicate should be destroyed as soon as no longer required.

5.2 Do we need to retain every version?

Retaining multiple versions is only applicable in certain cases. It depends on the nature of the document and whether any significant amendments were made to each version to warrant retaining it.

If multiple versions of a document do need to be retained, they should be saved as separate documents, and the title should clearly show that is a new or separate version.

5.3 Where should we store records?

All Authority records should be created in or transferred into shared systems, do not store core business records in OneDrive or Outlook. They should be saved as early as possible, so that they are immediately made available to share as appropriate.

5.4 Email

Emails often provide significant evidence of actions and decisions. However, this does not mean you should retain every email ever sent or received. Best practice

requires a continuous process of reviewing and weeding. Your email is not accessible to other staff, so you must not retain important records in Outlook.

Transfer emails required as evidence of business activities to shared systems (e.g. SharePoint) as soon as possible. Delete emails that are not required.

6. Suspending disposal of records

The decision to interrupt a planned disposal and subsequent review of the information will be alerted to the Information Asset Owner and the Data Protection Officer.

6.1 Suspensions

The UK Covid-19 Inquiry has been set up to examine the UK's response to and impact of the Covid-19 pandemic and learn lessons for the future. Destruction of Covid-19 related records is suspended until further notice.

7. Training and awareness

As all Authority employees are involved in creating, maintaining, and using records it is vital that they all understand their records management responsibilities as set out in this policy.

Managers must ensure that all their staff are aware of their obligations regarding Data Protection, Freedom of Information, and Records Management. Training on Information Governance and Security is mandatory for all staff.

Non-compliance could result in the Authority being put at risk of reputational damage, loss of confidence in the Authority, legal challenge and ultimately could lead to our service users being put at risk.

Actions or neglect leading to a breach of this policy by an employee could result in disciplinary action.

Document Control

Document owner	DPO, SIRO
File Location	Information Governance
Current review	April 25
Next review	March 26
Approval by	SIRO, DPO, CISO
Approval date	

Version	V1.0 This policy has been created following recommendations from the recent IG Audit
Relevant Officers	
SIRO	Director of Resources
DPO	Information Governance and Compliance Manager/Data Protection Officer