



Records Management Policy

**Approved
June 2026**

**Approved by
Senior Leadership Team**

Procedure Title	Records Management Policy
Document Owner	Head of Information Management and Library Services

Procedure Effective From	June 2026
Next Review Date	June 2031

New College Durham is committed to safeguarding and promoting the welfare of children and young people, as well as vulnerable adults, and expects all staff and volunteers to share this commitment.

If you require this document in an alternative format and/or language, please contact records@newdur.ac.uk

We review our policies regularly to update them and to ensure that they are accessible and fair to all. All policies are subject to equality impact assessments which are carried out to determine whether the policy has, or is likely to have, a different impact on those with protected characteristics. We are always keen to hear from anyone who wants to contribute to these impact assessments, and we welcome suggestions for improving the accessibility of fairness of this and all College policies.

Other policies and procedures mentioned in this document will be published internally and externally in these locations:

[Website](#)

This policy has been assessed for its compliance with the principles of the OIA Good Practice Framework.

To make suggestions or to see further information please contact:

Information Management and Library Services

records@newdur.ac.uk

Contents

- 1. Objectives 4
- 2. Responsibilities 4
- 3. Relationship with existing policies and standards 5
- 4. Definitions 6
- 5. Policy and Guidance..... 6
 - a. Fileplan and Records Retention Schedule (RRS)..... 7
 - b. Information Asset Register 8
 - c. Paper Records..... 8
 - d. Access Controls..... 8
 - e. Authentication 8
 - f. Disposition 8
 - g. Preservation..... 9
 - h. College Archive 10
- 6. Evaluation and review..... 10

1. Objectives

This Policy is intended to facilitate the effective management of the College's records and archives as a source of evidence and information. It encompasses records in all media and in all parts of the organisation and includes all the information created, received and maintained by staff of the College in the course of their work. This Records Management Policy can also be considered an Information Management Policy for the purposes of compliance with relevant standards.

The Policy objectives are to ensure that:

- Adequate records of the College's activities are created;
- Appropriate and efficient access to these records is provided for all authorised users;
- Records required for business, accountability or cultural purposes are retained and remain usable for as long as they are needed;
- Records of long-term value are identified and preserved as archives;
- Other records are confidentially destroyed when no longer required; and
- Employees are aware of what constitutes best practice in records management.

2. Responsibilities

The College has a responsibility to ensure its records are maintained in accordance with legislation concerning the subject matter of those records and concerning their accessibility. Responsibility for ensuring compliance with this Policy lies with the Corporation and the Senior Leadership Team.

The Senior Information Risk Owner (SIRO) for the College is the Deputy CEO. The SIRO is responsible for ensuring information and records management is recognised as a core function of the College.

The Academic Registrar is responsible for this policy and for developing and implementing consistent records systems that work across the College and providing records management advice to all departments.

The Information Management Team is responsible for implementing and maintaining retention mechanisms, maintaining associated record-keeping guidelines; promoting compliance with the provisions of the policy and guidelines and providing records management advice to all departments.

Where a legal statement is required to assert that information provided from a College Records System is genuine and accurate, the SIRO or Academic Registrar may be called upon to provide this statement.

Data, System and Site Owners are responsible for ensuring they understand the importance of effective records management and for applying the retention and security requirements of their records. They should also monitor the quality of the records with an eye to business risk and conformity with applicable standards.

All staff are responsible for maintaining the accuracy and completeness of the records they create and use. Compliance with this Policy and any associated procedures is compulsory for all staff employed by the College. A member of staff who fails to comply with this Policy may have their actions reviewed under the College's Competence Procedure or may be subjected to disciplinary action under the College's Disciplinary Procedure. It is the responsibility of all managers to ensure that staff are made aware of the existence of this Policy and its content.

ICT and Systems are responsible for the implementation of agreed technical controls to manage electronic records and the Information Management team will liaise with these teams to provide a comprehensive service.

3. Relationship with existing policies and standards

This Policy has been formulated within the context of the following College documents and associated guides available from the website and intranet:

- Data Protection Policy
- Freedom of Information Policy
- M365 Policy
- Information Security Policy
- ICT Disaster Recovery Plan
- ICT Digital Asset Policy

This Records Management Policy will seek to facilitate compliance with BS ISO 15489-1:2016 Records Management; BS ISO IEC 27001:2022 Information Security; and the Lord Chancellor's Code of Practice on the Management of Records under s46 of the Freedom of Information Act 2000 (2012 ed.).

The College will seek to comply with BS10008:2020 Evidential Weight and Legal Admissibility of Information Stored Electronically. This will be for scanned or uploaded records held in College systems (ie artefacts rather than data) that are required to evidence business transactions that will be required in the event of an audit by a funding or regulatory body.

The College will seek to comply with requirements stipulated by funding bodies and external institutional review bodies, especially where these relate to audit requirements.

Compliance with this Policy will facilitate compliance with other information-related and records legislation such as:

- Freedom of Information Act 2000
- General Data Protection Regulation (GDPR; UKGDPR)
- Data Protection Act 2018
- Public Records Act 1958

4. Definitions¹

Data is often defined as ‘raw facts’ and information is often defined as ‘processed data’ but for the purposes of this Policy the terms will be considered synonymous.

A **record** is “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”; a record provides “evidence of a transaction and its terms...reference material for the organisation of facts, background, prior actions and ideas to be used in decision making processes...evidence of enabling compliance with legislative or professional requirements”.

A **document** is “an object which can be treated as a unit”; where the context or content is not a consideration.

An **archive** is a collection of records stored for longer than their useful lifetime for historical purposes.

An **Information Asset** is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently (eg. a database).

College records consist of all documents, databases and any other collection of information fitting the above definition of a record.

5. Policy and Guidance

The College will manage its records in the most effective way to ensure a consistent approach is maintained. It is expected that records will be captured in the most appropriate system as identified in the College Fileplan (see action 5a).

¹ Definitions in quotation marks are from BS ISO15489:2016 Records Management

The College is committed to creating, capturing, using and storing records electronically where possible. The use of electronic systems must maximise the evidential weight of records held, especially those which have been scanned.

OneDrive, Network Shares, Outlook and Teams channels are not records management systems and information held in these and other MS tools should be filed appropriately into the system where the data owner has specified their records should be held. The retention on these data stores is shorter than that which may be required for legal or regulatory purposes. For more detail please see the M365 Management Policy.

It is expected that any new records management system or database that will be used to process personal data has had a data protection impact assessment.

The following are elements of the College Records Management Policy and any procedures therein should be followed.

a. Fileplan and Records Retention Schedule (RRS)

This resource consists of a list of categories against which records are classified². It is based upon models created by JISC and is reviewed when the JISC models are updated. All current College records are classified therein to comprise the Fileplan.

In addition, information is included detailing the length of time for which the College undertakes to keep each class of records. These retention schedules are based on legislative and funding body requirements as well as operational requirements and are subject to change. Changes will be applied by the Academic Registrar in consultation with the relevant School or business area.

Retention periods apply to the record and to any associated index data held with the record. Audit trail data should be held for at least as long as the record but may be held longer.

Processes must be established by departments to ensure retention periods listed here are adhered to. These processes should be documented and published internally. In these processes requirements for compliance in relation to section 3 (above) must be met.

This resource also contains information on the lawful basis for processing where the records contain 'personal data' or 'special category data' and the Privacy Notice where

² The College uses the JISC 2006 model Business Classification Scheme, cross referenced with the 2009, 2019 and 2025 versions

the information is communicated. The Fileplan is also the Record of Processing Activity (ROPA) for the College as required by the UK GDPR.

b. Information Asset Register

This resource is a register of all College systems which contain data. It forms part of the College's ROPA for the purposes of compliance with data protection legislation and is managed by the Information Compliance Co-ordinator.

c. Paper Records

The scanning and indexing of paper records should be carried out according to user guides supplied by the owner department. Where the physical condition of the document is compromised this information should be captured if it affects the legibility of the content.

Manual security must be applied to paper records. The department should maintain a record of documents or files signed out of the secure storage and consideration should be given by the Data Owner of the physical security/safety of the records. The physical safety considerations must include whether records are at risk of fire or water damage as well as theft or accidental loss.

d. Access Controls

Access to College records is determined by the Data Owner for those records. Access permissions on SharePoint Sites are the responsibility of the Site Owner.

e. Authentication

If proof is required that documents or data are genuine College records, the Academic Registrar can provide an authenticated version which can be certified as genuine.

Where a legal statement is required attesting that information provided from a College System is genuine and accurate, the SIRO will provide this statement.

f. Migration

Where records are transferred between systems the data owner must ensure a checking process is undertaken to establish the location and quality of the transferred records is appropriate and that any metadata accompanying the records is accurate.

g. Redaction

Where redaction is used the tools must sufficiently occlude the data redacted. A copy of the unredacted record should also be held. Any tool must ensure that data is held securely.

h. Disposition

Records must be disposed of according to the retention schedules, wherever they are held.

Disposition may be automated or by management sign off. On request from the Data Owner, the Information and Records team can put a 'hold' on records for disposal if a record is the focus of an on-going Data Protection or FOI request or because the records concern an on-going legal case.

Any records or original paper copies should be disposed in a secure and confidential way using the appropriate consoles provided by Estates. Any service provider used by the College to dispose of confidential waste must be a member of the British Security Industry Association (BSIA) or must be able to prove compliance with *BS8470 Secure destruction of confidential material*.

g. Preservation

The College undertakes to preserve records for the duration of their retention and to preserve any archives for as long as items are required.

Records electronically held will be more vulnerable to preservation issues such as format obsolescence; this may render a record unreadable before its retention expires. The College recognises that these record types include:

- Assessment Board Records, Transcripts
- Academic Regulations, Programme Specifications
- Academic Board Papers
- Corporation Papers & Legal Framework, Register of Seals
- Estates Records (property ownership, maintenance of long-term assets, H&S File)
- Insurance Policies
- Legal Advice with Precedent
- Health and Safety Records (Policies, H&S Committee papers, accident records, exposure monitoring, health surveillance, safety equipment specification and maintenance)
- Pension Scheme Contributions and Correspondence

- Staff Files
- Staff disciplinary records indicating permanent sanction
- Industrial Relations Management
- DPIA, Register of Processing Activity (RoPA), Compliance documentation
- Contracts Register

h. College Archive

The content of the College Archive is managed by the Academic Registry. The Archive contains materials of historical interest preserved for posterity.

6. Evaluation and review

The performance of this Policy is reported on annually and the policy is formally reviewed every five years by the appropriate Corporation committee.

In addition, the effectiveness of this Policy is monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.