New College Durham

Academic Registry

Records Management Manual

Contents

1. Introduction to Records

a. Policy and Compliance

New College Durham is committed to a records management programme which enables compliance with legal and regulatory requirements and compliance with established standards for records management, especially *BS/ISO15489* and the *Lord Chancellor's Code of Practice on the Management of Records under s46 of the Freedom of Information Act 2000*. The College has a Records Management Policy, an M365 Management Policy, a Freedom of Information Policy, a Data Protection Policy and an Information Security Policy published on its website.

The College is committed to electronic recordkeeping and where this is possible records should be held electronically.

b. Records Management Systems at New College Durham

Within the College, the records management systems incorporate all Registered Departmental SharePoint repositories[1], network shares, paper files and Information Systems containing uploaded files. Database records are also held in College Systems.

Where records are stored there should be documentation available to outline the way in which these systems will be managed to conform to the records management policy, specifically the College's records retention schedules and the requirement to create authentic records that have integrity. Guides should include processes for capturing metadata, preferred storage formats and requirements for version control.

To ensure the quality and value of electronic records all systems containing scanned images of student or staff records are audited for compliance with *BS 10008:2020 Evidential weight and legal admissibility of electronic information*. Documentation required to prove compliance with this code, including the retention of superseded compliance documentation will be held by Academic Registry as part of the Information Asset Register. Compliance audits will be carried out periodically to reflect changes in the way documentation is stored.

2. Keeping College Records

The College manages its records in the most effective way to ensure a consistent approach is maintained. This section of the manual will describe how the College enables records to be managed systematically.

a. Capture

Each time an activity is undertaken in the course of business, an evidential trace is

[1] This does not include OneDrive or SharePoint Sites which are 'spun up' with Teams sites. For clarification see the M365 Management Policy.

created and someone must make a decision about whether it needs to be captured as a record. The College considers that if the activity undertaken is a business activity[2] and the document or file is not usually disposed of under standard operating procedures (Appendix A), it must be captured as a record. This should be done by saving the document or file into the location specified in the fileplan or entering it as information into another College Database.

If the record cannot be stored electronically it should be held in paper copy and the Academic Registrar should be informed of its location.

If the business activity creates a record that can be captured directly (eg. an e-mail, a letter, or a piece of CCTV footage) then this should be done. If this cannot be done then the event should be documented.

The scanning, indexing and transfer of files, documentation and correspondence should be undertaken according to the user guides the department has provided. This is to protect the integrity and authenticity of the records.

b. Classification and Indexing

i. Business Classification Scheme (BCS)

This is a list of functional categories into which College records can be placed. Each category relates to an activity undertaken by the College. The BCS will rarely be changed and any changes will be made by the Academic Registrar as the result of a review of the business functions.

ii. Fileplan

This is a list of all College records listed within the categories referred to in the BCS. The Fileplan will be amended as a result of changing activities, the need to provide new services or new regulatory obligations. The College Fileplan is managed by Academic Registry.

Responsibility for adding files will lie with individual departments when new individual 'case files' need to be opened (examples include Personal Files, Student Files, Complaints Files). These should each be given a unique reference. Each department is responsible for keeping a log of these unique references.

iii. References and Indexing

Indexing is adding metadata[3] to a document to ensure it is filed correctly. Within some systems this involves the user filling in text boxes. Indexing will take place when any document is filed within a document management system.

---

[2] An activity covered by the Business Classification Scheme (see section 2.b.i.)

[3] Metadata is information attached to the record to allow it to be indexed (eg. date created, file reference, author)

Care should be taken to ensure information about a record is not lost when it is indexed. Therefore any information about the physical condition of the document (for example something which might help explain why a scanned image is partially illegible) should be captured by the indexer.

References should be added to internally produced documents.

c. Storage and Handling

i. Storage of electronic records

Storage environments should be appropriate to the format and security required by the record. Records stored in network shares and in College database systems will be covered by the network management provisions of the Information Security Policy.

ii. Storage of paper copy records

Confidential records or personal data that is not held electronically must be held in lockable filing cabinets or tambour cupboards.

d. Access Controls

i. Security and Permissions

Access to College records is determined/authorised by the Data Owner for those records. Access to SharePoint sites will be administrated by the nominated system or site owner.

ii. Tracking

Paper records cannot be 'backed-up' or audited in the way an electronic record can. Each department will be expected to ensure that physical access is only given to authorised users working in the area where the records are kept and if a file is taken outside the working area a log of the loan should be kept in a register that can be inspected on request by any auditor.

iii. Authenticating electronic records

If proof is required that a record is a genuine printout or export from a College system, Academic Registry can provide an authenticated version which will be signed and certified as genuine. This is dependent on the reliability of the operating procedures for the system.

The Academic Registrar will comment on any difference in formatting between the electronic document and any printed or exported version.

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

e. Retention

The College keeps a list of the lengths of time for which records will be held. These retention periods have been approved by the Senior Leadership Team and are listed in the Fileplan. They will be administrated and applied by the Information Compliance Co-ordinator and the Data Owner.

The College will ensure that consultation takes place with regulators and funding bodies to ensure that retention periods are set appropriately.

The Academic Registrar will also evaluate the status of the schedules on an ongoing basis to ensure legal and regulatory requirements are followed. Any major amendments to the retention schedules is approved by the Senior Leadership Team.

Backup records will be retained for the period of one year and may contain records that are in the process of disposal. The email backup is only held for 6 months and any email still held in Outlook that is over 2 years old will be deleted.

f. Disposal

Any records or original paper copies should be disposed of in line with the College's environmental policies**.** 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.*

The Information Compliance Co-ordinator 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. The Information and Records Team will be responsible for checking with the Senior Leadership Team regarding the status of on-going legal cases.

g. Disaster Preparedness

Electronically held records will be covered by the disaster recovery provisions of the College Information Security Policy.

The loss of paper records should be appropriately risk assessed by the department holding them before a decision is made to either improve the security of the storage unit in which they are stored or to migrate the records to electronic format. In the event that a record must be held in paper copy to retain its admissibility or integrity, appropriate fireproof and waterproof equipment must be procured if needed.

h. Preservation

In its Records Management Policy, the College undertakes to preserve records for the duration of their retention and to preserve any archives for as long as items are required. Paper records will not need significant steps taking to preserve access to them but the Information and Records Team will monitor the conditions under

which paper records are created and stored and will advise on any requirements for preservation.

Records held in document management systems will be more vulnerable to preservation issues such as format obsolescence; this may render a record unreadable before its retention expires. The Information and Records Team will ensure that the condition of electronic records is monitored and that any steps necessary are taken to preserve the integrity and accessibility of electronic records.

i. When other Organisations are Responsible for College Records

The College may, from time-to-time, ask an external party to hold or process records on its behalf. Terms and Conditions should be imposed on these outsourced service providers requiring them to follow College Policy on Data Protection, Freedom of Information and Records Management.

j. Management of the College Store and Archive

The College records store is used for the storage of paper records that are no longer active but have not yet reached their destruction date. These are kept in boxes in the College Records Store located in the Sports Building.

In order to submit records to the store, a department must order storage boxes and make a list of the contents along with the disposal date for the records within. One copy of the list should be sent to the Information Compliance Co-ordinator and a second copy should be attached to the inside of the box. The Information Compliance Co-ordinator will then number the boxes and arrange for their collection and transfer to the store.

If any records have to be retrieved from the records store, the Information Compliance Co-ordinator should be informed via e-mail and delivery will be arranged. Two to three working days should be allowed for delivery.

The College archive is managed by the Academic Registrar. Periodically, departments may submit non-records material to be placed in the archive. The Information and Records Team may also admit records to the archives that have surpassed their retention within the College in line with guidelines on public record-keeping from the National Archives. Contents of the College archive will be passed to the County Records Office for permanent retention as appropriate.

Appendix A: Standard Operating Procedures

The following is a list of types of information that can be disposed of by any member of staff as required in the course of their duties and should not be placed into storage.

- Drafts and working papers or documents
- Material collected for research or reference purposes
- Personal and inconsequential e-mails
- Copies of internal documents, correspondence and e-mails provided 'for information'