Information & Records Management

@ New College Durham

- What is a College record?
- How do I access archived information or data?
- What should I save and where?
- How long do I need to keep my records for?
- How do I dispose of records?
- How secure do my records need to be?

New College Durham

DOCUMENT HISTORY[1]

Consultation Detail	Approved by	Date Approved	Details of Amendment/ Review
Records; ICT; Admin; Finance	Strategy & Resources Committee	7 October 2015	Full review

---

[1] Changes to this manual must be approved by the Information, Records and Projects Manager.

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 , a Freedom of Information Policy, a Data Protection Policy and an Information Security Policy published on its website.

b. The Records Management Systems at New College Durham

Within the College, the records management systems incorporate all paper systems, network shares and the eRMS[2].   Database records are held in College Systems like Unit-e and SFP. Systems in which records are held as scanned images are

IDOX EDRMS
Version One
InTend
Cohort
Podiatry Patient Management System
Smart Assessor

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

Where records are stored in shared network drives there should be documentation available to outline the way in which these systems conform to the records management policy, specifically the College's records retention schedules.

To ensure the quality and value of electronic records all systems containing scanned images of records are audited for compliance with the *BS 10008:2014 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of electronic information.*   Documentation required to prove compliance with this code, including the retention of superseded compliance documentation will be held in the relevant section of the electronic records system.   These 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 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[3] and the document or

---

[2] Electronic Document and Records Management System, currently comprising IDOX DMS and DRM.

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

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 eRMS or entering it as information into another College System.

> If the record cannot be stored electronically it should be held in paper copy and the Information, Records and Projects Manager 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 in line with College procedures.   Telephone calls and meetings are an example of this kind of activity and should be documented in line with the College Telephone Procedure and the College Meetings Guidelines.

College Templates must be used for the creation of electronic documents in line with the Policy on Standardisation of College Documents.

> Each member of staff is responsible for dealing with their own correspondence and work allocated to them and must check their email inbox and workflow queues on a daily basis.

The scanning and indexing of documentation and correspondence should be undertaken according to the user guides the department has provided.   The scanning process will be audited for quality control purposes[4].

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 Information, Records and Projects Manager 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 each time the College needs to create new records as a result of changing activities, the need to provide new services or new regulatory obligations.   Any changes will be made by the Information, Records and Projects Manager.

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 using a database or spreadsheet.

The current College Fileplan is available from the Information, Records and Projects Manager.

---

[4] See the Quality Control Sampling Procedure (Appendix B)

iii. References and Indexing

Indexing is adding metadata[5] to a document to ensure it is filed correctly. Within some systems this involves the user filling in text boxes. Within Version One indexing is done automatically using data capture software. Indexing will take place when any document is filed within a document management system.

> Responsibility for ensuring a document is indexed lies with the person who receives or is allocated the correspondence by an administrator (in the cases of incoming post and e-mail) and the person who creates the document (in the case of internal materials).

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. The description field should be used where no other appropriate field is available.

References should be added to internally produced documents as outlined in the Policy on Standardisation of College Documents.

c. Storage and Handling

i. Storage of electronic records

Storage environments should be appropriate to the format and security required by the record. Storage media will be appropriate to the relevant system, disk and tape media will be used for backups. CD and DVD are not appropriate media for the storage of records.

Records stored in network shares and in College database systems will be covered by the network management provisions of the Information Security Policy. Records held in systems hosted externally may pose a greater business continuity risk.

Records may be saved into any format which can be accepted by the system.

> Staff should not store College records on a C: drive or in the 'home' folder provided on their Z: drive. The Z: drive may still be used to store personal documents but should not contain any files that may be required by the College at any time.

Shared folders may be set up to store some records and databases. Requests for shared folders should be submitted using the ICT Helpdesk.

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.

---

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

d. *Access Controls*

i. **Security and Permissions**
Access to College records is determined by the Data Owner for those records. The Information, Records and Projects Manager is responsible for allocating appropriate permissions to the IDOX EDRMS and network shares in consultation with the relevant Director.

The Information Co-ordinator will ensure access permissions are created, suspended or removed as appropriate within the IDOX EDRMS. This will be done according to the information access provisions of the College Information Security Policy.

Access to other systems will be administrated by the system owner.

ii. **Tracking**
The IDOX EDRMS will hold an auditable log of the activities/access history of each record held in it.

Paper records cannot be 'backed-up' 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 the IDOX EDRMS, the Records Manager can provide an authenticated version which will be signed and certified as genuine.

The Information, Records and Projects Manager 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 SIRO 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 Executive Group and are listed in the Fileplan. They will be administrated by the Information, Records and Projects Manager who 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 should be approved by the Senior Executive Group.

The head of each department will be responsible for ensuring the retention rules are applied to records held within the department. The College will ensure that consultation takes place with regulators and funding bodies to ensure that retention periods are set appropriately.

 Guidance on the Storage and Retention of Teaching Records is available (Appendix C).

In addition 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.   *Disposition*

i.   **Disposal of records**
Records must be disposed of according to the retention schedules, wherever they are held.   The disposal of records should be authorised using the Authorisation for Destruction Form (Appendix D) and records should only be disposed of once the form is appropriately authorised.   The authorisation should be sent to the Information, Records and Projects Manager to be filed.

ii.   **Disposal of paper copy of electronic records**
Any records or original paper copies should be disposed of in line with the College's Confidential Waste Disposal Guidelines**.**   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, Records and Projects Manager 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, Records and Projects Manager will be responsible for checking with the Senior Executive Group regarding the status of on-going legal cases.

g.   *Disaster Preparedness*

Records stored in the eRMS and in College database systems 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.

In the event of a 'disaster' the College will follow procedures outlined in the Disaster Recovery Plan and the ICT Business Continuity Plan.   The Information, Records and Projects Manager and the Head of ICT will be asked to report to the Disaster Recovery Team and identify the loss of any business critical records and assess the effect of the disaster on College record keeping systems.

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, Records and Projects Manager 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 ICT department 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 from CPU 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 Records Assistant and a second copy should be attached to the inside of the box. The department will then put a request on the ICT Helpdesk. The Records Assistant 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 Records Assistant 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 Information, Records and Projects Manager. Periodically, departments may submit non-records material to be placed in the archive; these will be appraised by the Principal. The Information, Records and Projects Manager may also admit records to the archives that have surpassed their retention within the eRMS 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.

k. *Support Service*

Any request for assistance with IDOX or network shares, including changes to user permissions, settings and technical help must be submitted via the ICT Helpdesk.

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.

- ◎ Calendars/Diaries (unless specified in the Fileplan)

- ◎ Drafts and working papers or documents

- ◎ Material collected for research or reference purposes

- ◎ Complements slips

- ◎ Personal and inconsequential e-mails

- ◎ Copies of internal documents, correspondence and e-mails provided 'for information'

- ◎ Copies of documents held in an electronic 'Course File' for the current year and no longer

  required

Appendix B: Quality Control

Batch Sampling Procedure

1. Quality sampling is undertaken by members of the ICT Department every month.   The following information is collected from a selection of random batches.   The following information is collected:

   Date of Check
   Date of Batch
   Name of Batch
   Comments on Acceptability and Quality

   In addition other observations may be made.   Non-compliances are followed up with relevant departments.   Details of contact and outcomes are logged.

3. The person who performs these checks must not select a batch of their own to check.

4. A log of the results of these checks is held as a record of system maintenance.

It is expected that records which are subject to audit or potential legal challenge be held in a system that will comply with *BS 10008:2014 Evidential weight and legal admissibility of electronic information.*

Appendix C: Retention of Teaching Records

Guideline for curriculum staff

This guideline is intended to supplement the College Records Management Policy and is based on best practice across the FE/HE sector, advice from the QAA and relevant awarding bodies.

The approved College retention periods for teaching records and student work are as follows:

Retention for student basic record, assessment marks (from 2010) and final results	Indefinitely (held on Unit-e)
Student Work (Assessments, Course Work & Exam Scripts)	Current Academic Year + 1
Records of Assessment Verification (incl. samples of verified work)	Current Academic Year + 3
Records of Examination Verification (incl. samples of verified work)	Current Academic Year + 5
Records of Assessment Marks (not held on Unit-e), Methods and Assessors	Current Academic Year + 6
External Verifier Reports and Action Plan (usu. HE)	Current Academic Year + 10
Student Tutorial, Progress or Personal Files	Attendance on Course + 6
Course Review Meetings	Current Academic Year + 6
Teaching Events/Visits	Current Academic Year + 1
Course Statistics	Current Academic Year + 5
Course Feedback and Review	Current Academic Year + 5
Course Materials	Life of Programme/Course
Course Development/ Accreditation Records	Life of Programme/Course + 10

Course Work and Assessments

Student work should be offered back to the student at the end of each academic year.   If not collected it should be boxed up for storage and disposal at the end of the next academic year.   A small sample (usually work submitted for verification purposes) should be retained for quality purposes and may be scanned into the Assessment File. If students want to retain examples of their work for later use (as the basis of an appeal for assessment review or any other reason) then they should be informed that they are responsible for taking ownership of it, and subsequently producing it, after the assessment process is over.

Examination scripts

Exam scripts should be retained for six months following the publication of results and then securely disposed of.   A small sample (usually those entries used for verification purposes) should be retained for quality purposes. Any script which is still the subject of an ongoing procedural or legal challenge should be retained until that process is complete.

Appendix D: Authorisation for Destruction Form

Authorisation for Destruction

The records listed below are recommended for destruction according to the College's retention schedules.

Date: Depositor:

Description of File	Special Notes (if any)	Ref	Date Disposal Due	Mark as D or H*	RM Action

Please indicate on each line **D for the records you approve for disposal, or **H** if the records are due for destruction according to the schedules but you want to place the disposal on hold.   If so, please indicate the reason for their continued retention.*

Authorisation for destruction: _____   Signature

                                                        _____   Date

Once Authorised and the disposals implemented, this form must be sent to the Information and Records Team to be filed.

For more information on the College Records Retention Periods please refer to the list of schedules on the Intranet, which can be found under Departments/Information and Records Management/lists and registers.