INSPIRING. TRANSFORMING. ENRICHING.

POLICY TITLE

RECORDS MANAGEMENT POLICY

Academic Year: 2013/14 onwards

Target Audience:

Governing Body
All Staff and Students
Stakeholders

Summary of Contents:

Good records management allows the College to satisfy the needs of corporate accountability, statutory obligations and audit requirements. This policy sets out in broad terms how the records the College produces are managed effectively.

Enquiries: Any enquiries about the contents of this document should be addressed to:-

Title: Information Officer

Campus Address: Bangor Campus, Castle Park Road, Bangor, BT20 4TD

Tele: 028 9127 6600
Fax: 028 9127 6601
E-mail: sharvey@serc.ac.uk

Final approval by:

CMT - 1 October 2014

Governing Body – 19 February 2013

Policy Number: 017-2014

First Created: February 2013
Last Reviewed: June 2016
Review due: May 2018

Related Documents:

SERC Publication Scheme
SERC Retention Schedule
Freedom of Information Policy
Data Protection and Data Security Policy
Freedom of Information (FOI) SOP
Data Protection Subject Access Request SOP
ICT Security Policy
Acceptable Use Policy
ICT Security SOP
Freedom of Information Act 2000
Data Protection Act 1998
Environmental Information Regulations 2004

Superseded Documents (if applicable):

02-2013

Document Control Administrator

FOI Category:

FOI Class:

FOI Ref:

1.0 Purpose

SERC's compliance with the Data Protection Act (1998) and the Freedom of Information Act (2000) can only be efficient if there is an investment of time and resources in creating an organised and agreed Records Management system. Good records management allows the College to satisfy the needs of corporate accountability, statutory obligations and audit requirements. An approved records management system reduces the risk of records being lost, damaged or accessed by unauthorised personnel. In addition, effective records management is an efficient management of resources, helping to reduce costs, avoid wastage and improve retrieval rates in response to Subject Access and Freedom of Information requests. SERC is committed to ensuring that the records it produces are managed effectively from the point of creation to their ultimate destruction or transfer to permanent preservation. This policy statement sets out in broad terms how that commitment will be put into practice.

Definition of a Record

Records are the evidence of the College's actions and decisions.

A record is any information created or received and maintained as evidence of business by a person or organisation. These records can be paper-based or electronic. Some records are essential for on-going work, such as a student electronic Individual Student Learning Agreement (e-ISLA) or Electronic Personal Training Plan (e-PTP). Some records are required to be archived for a statutory period, such as financial records. As a public authority, the College also has a duty to keep some records simply as evidence of what was done and why..

2.0 Scope

This policy applies to all records created and received by the College. These records will include all student and staff files, invoices, correspondence, policies, minutes of meetings etc. Its provisions extend to all staff and any students conducting business on behalf of the college.

3.0 Roles and Responsibilities for Records Management and Organisational Responsibility

The Records Manager has responsibility on behalf of the Principal:

- To ensure the College is aware of changes in legislation which impact on how we manage our records.
- To update relevant SERC policies and procedure to reflect changes in legislation.
- To establish, monitor and review a College Record Management system to ensure the correct classification, storage, security, destruction, archiving and retrieval of information
- To develop, co-ordinate and deliver a College wide training and awareness programme on DPA, FOI and Records Management and communicate staff responsibilities applicable to regarding compliance.
- To be the contact point for all Freedom of Information and Subject Access Requests, liaise with all responsible owners and issue a response in compliance with the relevant Act(s) of legislation.

4.0 Legal Obligations

As a public authority SERC must manage its records in accordance with Acts of legislation. The Information Commissioners Office (ICO) regulates the application of these Acts and will take action where a breach occurs.

Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act (2000)

Section 46 of the Freedom of Information Act (2000) states that the Lord Chancellor will issue "a Code of Practice providing guidance to relevant authorities as to the practice which it would, in his opinion, be desirable for them to follow in connection with the keeping, management and destruction of their records."

The Public Records Act (NI), 1923

The Public Records Act (1923) established The Public Record Office of Northern Ireland (PRONI) as the place of deposit for public records, created the roles of Keeper and Deputy Keeper of the records as well as defining what public records actually are.

Freedom of Information Act (2000)

The Freedom of Information (FOI) Act 2000 covers any recorded information i.e. printed documents, computer files, letters, emails, photographs, sound and video recordings held by the College. The main principle behind the FOI legislation is that the general public have a right to know about the activities of public authorities unless there is a good reason for them not to. Information may only be withheld if there is an absolute exemption or the public interest test considers that the public interest in maintaining a qualified exemption outweighs disclosure.

The College has a legal obligation to provide information through an approved publication scheme and in response to requests. The College must respond to a request within 20 working days.

Publication Scheme

The College must also produce a "Publication Scheme" which should list classes of information about activities which are in the public domain and which the College has published or intends to publish. In this context, "publish" means to make information routinely available. It must also make clear how the information described can be accessed, the medium in which it is available and whether or not charges will apply.

These descriptions are called "classes of information". The scheme is not a list of the actual publications, because this will change as new material is published or existing material revised. It is, however, SERC's commitment to make available the information described.

The Publication Scheme is available on the SERC website.

Disposal of Records Order (1925)

The Disposal of Records Order (1925) sets out how PRONI and government departments should deal with the disposal of public records once their business need comes to an end. Records management is ultimately a matter of risk management, and the College must

control the risks associated with the retention and disposal of records. The ICO and PRONI require the College to develop an NI Assembly approved Retention Schedule which identifies the classes of information held, how long the record should be archived and retained and what the final action will be e.g destroy, transfer to permanent archive. A Retention Schedule is a list of record types or 'classes' with the following information:

- Functionality
    - The general category of information
- Record Type
    - What the record contains information on and how it is used
- Retention period
    - How long to keep the records for
- Statutory authority or guidelines
    - Is there a legal or departmental requirement to retain the information
- Final Action
    - What we do when the record reaches its 'disposal date'

The majority of records created by the College do not have sufficient importance to warrant permanent retention and should be destroyed at specified times according to the agreed Retention Schedule. The destruction of any record produced by the College in the course of its activities should only be carried out after it is has been assessed for legal, administration or archival retention requirements. Confidential records must be disposed of securely and safely and an audit trail must be kept of such decisions.

Data Protection Act (1998)

Under the Data Protection Act (1998) the College is a registered data controller, registration number Z6477199. The College is required to process and safeguard all personal data in accordance with the eight Data Protection principles set out in the Act.
The College recognises the importance of protecting its information assets and, in particular, the information relating to its staff, students and other individuals in whatever form that information is held.

The College functions require us to obtain, process and manage certain information about individuals/organisations to enable us to provide a high level of service being requested, for example:

- course programme administration
- providing education and training
- obtaining results for courses and examinations
- administration of student awards and fees
- staff recruitment, salaries and travel allowances paid, annual leave calculation, membership to pension schemes arranged
- facilities provided
- legal obligations to funding bodies and legislation complied with
- Returns to Department of Learning

The College is required by the Department for Employment and Learning to ask for the following information for statistical purposes: marital status, racial group, religion, employment sector, and employment status.

All data, whether held electronically or manually, must be kept securely and not disclosed unlawfully.

The sixth principle gives individuals including SERC staff, students and related third parties to access personal data about them which is being held by the College, either electronically or in a relevant filing system, to check that it has been fairly obtained, that it is accurate, and to have such data corrected where necessary. It also recognises the right of a data subject to withdraw consent to the processing of personal data where such processing could cause them significant damage or distress.

Environmental Information Regulations (2004)

The Environmental Information Regulations (2004) require public authorities to take reasonable steps to organise and keep up to date the environmental information which it holds and which is relevant to the public authorities function. It gives members of the public the right to access 'environmental information' held by public authorities. The College must respond to a request within 20 working days.

5.0 Classification of types of records – format, confidential and non-confidential

There are three stages of the life of every record: it is created as a current/active record; it is maintained as a semi-current record with continued value for the College e.g reference purposes or audit requirements; and it is destroyed or transferred to permanent preservation when it becomes a non-current record.

6.0 Version control

As part of its record management policy, it is vital that the administrative journey of a policy is recorded. The final approval should indicate the level at which final approval of the policy rests and the date when the policy receives final approval. Policy Review should document any changes and whether it requires re-approval.

7.0 Risk management

6.1(b) of Section 46 stipulates that Records Management should be included in the corporate risk management framework. Information and records are a corporate asset, the loss of which could cause disruption to business. The level of risk will vary according to the strategic and operational value of the asset to the authority and risk management should reflect the predicted extent of disruption and resulting damage

Risk Management is about identifying what could go wrong and ensuring that appropriate procedures are in place to prevent these risks from occurring.

There are risks around records such as loss, damage or unauthorised access which need to be managed effectively.

Staff should ensure that all records, paper or electronic, are stored safely and securely. These provisions should be appropriate to the nature of the data or information held in the record, which can include:

Personal and sensitive data

The Data Protection Act requires the College to ensure 'appropriate technical measures' are in place around personal information. There are greater risks around 'sensitive'

personal information, which includes information about matters such as an individual's health, political allegiance or ethnicity therefore additional security measures will be taken.

Financial or commercially sensitive data

Mishandling of this information could have serious implications for the commercial performance and financial health of the College.

Storage risks include:

- **Loss**
  The loss of records through unauthorised destruction or accidental deletion or – more seriously – the loss of records which can result in unauthorised access (see below)
- **Unauthorised access**
  Records being viewed by unauthorised members of staff or the public resulting from accidental loss, user error (such as emailing or posting to the wrong recipient) or through malicious attacks to College's ICT systems.
- **Unnecessary retention**
  Records can be kept longer than they are required, leaving the College exposed to complaints of breaching the Data Protection Act
- **Damage**
  Paper and electronic records can be damaged or destroyed if storage locations are damaged by flooding or fire.
- **Obsolete format**
  Electronic formats can, by virtue of changes in software and technology, quickly become obsolete
  Steps to mitigate these risks should be put in place around their records by all Units and Schools. The procurement and implementation of new ICT systems holding information should include an assessment of how records will be stored.
  If the system is replacing another it should also provide a solution for the records held on the obsolete system.

Effective records management requires regular risk management activities including risk assessments on storage, security, retention of records. The College will require each School and Unit responsible for creation and storage of records to conduct annual risk assessments to ensure that records are kept secure and are retained for period of time detailed in the Retention and Disposal Schedule.

8.0 Record Storage and Security

The storage of records should allow easy and efficient retrieval of information but also minimise the risk of damage, loss or unauthorised access.

Security of both paper and electronic records, particularly those records deemed to be confidential or sensitive, is a legal requirement. Consequently, the College will require all record creators and processors to ensure that the following measures are adhered to:-

- All records are to be securely stored. Paper records to be locked in cabinets when not currently being processed.
- All electronic data will be securely stored on the College server infrastructure. Staff should upload documents to the SharePoint team sites and log out of/lock PC's which are not in use.

- All mobile devices should be encrypted to protect information in the event of theft, accidental loss or damage.
- Records must only be accessed by those staff or students that have authorisation to do so. For electronic records, system managers must regularly check permission levels and remove those who no longer require access to certain classes of information.
- Records must be created and stored as per College guidelines. Electronic record applies to those contained in documents, e-mail messages. Database or system records are created as per software design and as a consequence users have no control over the storage of records. However, all electronically stored records must be secured in terms of application of access permissions and must be backed up as per the College ICT Security Policy and SOP. Responsibility for backups rests with each College ICT Systems Manager.
- Certain records which are no longer current but required to be retained for a period of time may be transferred to an off-site storage facility. A tracking system will be established to authorise and control the movement and location of records so that they can be easily retrieved for reference or for the purpose of responding to information requests.
- Destruction of any record produced by the College in the course of its activities, including confidential records, should only be carried out where authorised.

9.0 Information Audit

The Records Manager will conduct biennial audit of SERC records. The audit will identify new records created and held by SERC, storage arrangements and permissions for electronic access. Significant changes to records held by SERC will be considered for inclusion on the Retention and Disposal Schedule.

10.0 Communication Plan

This Policy will be uploaded to the College Intranet for Staff and Governing Body reference, and is available to students and stakeholders upon request.

11.0 Review

This Policy will be reviewed (and amended if necessary) at least biannually or sooner if required to reflect changes in legislation or circumstances.

Appendix 1: Types of Records

Records which may be kept by the College for the following purposes:

- **Administrative value**
  Records which provide evidence of the actions, activities and decisions as a College;
- **Financial value**
  Evidence of the way in which money was obtained, allocated, controlled and spent;
- **Legal value**
  which will provide the source of the authority for actions taken by the College or individuals and show evidence of title, contractual obligations, duties and privileges;
- **Historical/archival value**
  Records which supply the corporate memory of the College and its legacy colleges. This will include records created for the purposes highlighted above, retained for historical reasons.
  Records are stored in a variety of location and formats:
- **Paper files**
  Paper records stored in offices or transferred to the College archive or third parties for storage;
- **Shared drives, personal drives and emails**
  Records produced day-to-day by staff at their computers and stored in network drives and email accounts provided by the College;
- **IT systems**
  Systems dedicated to holding information and data to support a specific business process, such as accounts payable, the library catalogue or student registration.
  A record will be in one of three states during its working life:
- **Current**
  This is an 'open' or 'working' record or file, still being updated and added to. These records will usually still be in the possession of their creator or owner.
- **Semi-current**
  This is a record which has been 'closed' but is used as a reference tool for administrative purposes.
  These records can be stored separately from their creator or owner, for example in the College archive or off site in third party stores or an electronic records system.
- **Archival**
  A record will be considered 'archival' if it is retained after its semi-current 'life' and selected for permanent retention in the College archive or an equivalent digital repository.
  A record may be considered to be confidential or non-confidential.
- C**onfidential**
  Information held by a public authority is subject to the provisions of the Freedom of Information Act 2000. The Act includes various exemptions to the disclosure of certain types of information, which may include *confidential* information as defined in this document.
- **Likely to be confidential**
  Records or information which contains personal information about a living individual e.g.
  Questionnaire or other data collected under a guarantee of confidentiality.
  - Correspondence or other documents which reveal the contact details or any financial details of a named living person, unless permission has been given to circulate the details.
  - Correspondence or other documents which reveal personal details or pass comments on a named living person.
  - Staff personnel records
  - Discipline records
  - Student records
  - Funding applications
  - Job applications
  - Interview notes
  - Admissions records
  - Redundancy records
  - Sick pay records

- Maternity pay records
- Income tax and National Insurance returns
- Wages and salary records
- Accident and incident reports
- Health records
- Medical records

- Information which, if made public before a certain period, may breach commercial confidentiality e.g.
  - Contracts
  - Tenders
  - Purchasing records
  - Maintenance records
  - Insurance records
  - Unpublished accounting records

- Records which may breach intellectual property rights e.g.
  - Unpublished research material, drafts and manuscripts.

- **Unlikely to be confidential**

  Records or information thereof which is already in the public domain e.g.
  - Mission statements
  - College Development Plans
  - Instruments and Articles of Governance
  - Regulations
  - Published directories
  - Internet websites
  - Published minutes
  - Published reports
  - Press releases
  - Prospectuses
  - Timetables
  - Presentation materials
  - Course guides and outlines
  - Publicity material
  - Blank examination papers (post exam)
  - Data which has been anonymised
  - Published surveys
  - Student and staff Magazines (Staff Express and Student Express)
  - Published circulars