RECORDS MANAGEMENT POLICY

REFERENCE: PL/CS/2018/004

Lead Officer	Principal and Chief Executive
Review Officer	Information Development Manager
Date first approved by BoM	20 December 2012
First Review Date	October 2015
Date review approved by BoM	21 June 2018
Next Review Date	May 2021
Equality impact assessment	Yes
Further information (where relevant)	

Reviewer	Date	Review Action/Impact
Information Development Manager	28.03.17	Review approved by BoM Audit Committee
Information Development Manager	21.06.18	Review approved by BoM

RECORDS MANAGEMENT POLICY FRAMEWORK

Contents

RECORDS MANAGEMENT POLICY FRAMEWORK

1. Policy Statement

Inverness College UHI is a publicly funded body that needs to be openly accountable for its decision making. Decisions need to be recorded in the form of records that are created and maintained to support and evidence past and present operations.

Efficient management of college records supports strategic decision making and informs organisational requirements to deliver the college strategic plan.

Inverness College UHI is committed to following the good practice guidelines laid down in the Records Management Code of Practice within Section 61of Freedom Of Information (Scotland) Act 2002 (FOISA).

2. Purpose of the Framework

Good records management helps staff to do their jobs more efficiently by ensuring information can be located when it is required. It promotes business efficiency and underpins service delivery by ensuring that authoritative information about past or current activities can be retrieved, used and relied upon in current business.

Legislation for data protection and freedom of information exists which gives the general public rights to access certain information. Without formal records management processes in place, it is difficult to ensure that the college complies with its legal obligations.

Scope
This policy applies to the management of all corporate college records irrespective of the technology used to create them or the business system or filing system in which they are stored. It covers records throughout their lifecycle from planning and creation through to disposal.

It includes records irrespective of where they are located and includes records managed on behalf of Inverness College UHI by an external body or contractor.

Records come in many formats but will be either in hard copy or electronic. The term electronic records, includes (but is not limited to) all business systems e.g. finance system, HR system, student records system, customer relationship databases, voicemail, photographs, film, cctv as well as the traditional word, excel, PowerPoint, Visio, email files etc.

Records Classification
Following completion of an information audit a records classification scheme for the college's corporate records was approved for use. The classification scheme should be used (where appropriate) to categorise both hard copy and electronic records. This will ensure consistent file naming conventions are used and a consistent approach is adopted to managing all college records.

Records Retention Schedule
A records retention schedule is in place and forms part of this policy, to ensure staff are able manage all records at departmental level. The records retention schedule will be revised from time to time as business requirements change so the current version will always be found on-line. This will be further developed as part of the UHI Tertiary Student Retention Schedule and further still when an electronic records management system is introduced.

An electronic records management system will be programmed to ensure all records created include a retention period. Where possible, this will be an automated process.

Destruction & Disposal of Records
Departmental managers/Team Leaders are responsible for ensuring corporate team records (both electronic and hard copy) are appraised annually in conjunction with the records retention schedule.

When an electronic records management system is in place, electronic records will automatically be removed from view when they are no longer current. The college Information Development Manager will liaise with departmental managers to ensure a final check is undertaken prior to deletion of records, once the retention period has been reached.

A process is in place to ensure appropriate disposal of all paper records.

3. Legislative Framework/Related Policies

- Freedom of Information (Scotland) Act 2002
- Code of Practice on Records Management (under section 61 of FOISA)
- EU Data Protection Regulation, UK Data Protection Act 2018
- Environmental Information (Scotland) Regulations 2004
- Health & Safety at Work Act 1974 (plus various associated regulations)
- Employment Law (various)
- Local Government in Scotland Act 2003
- The Public Records (Scotland) Act 2011
- Code of Audit Practice (Audit Scotland, March 2007)
- Information Security Policy
- Business Continuity Policy
- All college policies but specifically the Data Protection Policy & the Freedom of Information Policy

4. Responsibilities

4..1. Overall responsibility for records management lies with the Principal and Chief Executive. Managers and Team Leaders/Co-ordinators are responsible for ensuring:

- they have an understanding of the legislative and regulatory environment that applies to the activities and functions that are performed by their departments.
- records are created to record and evidence our business activities (this includes work undertaken by permanent staff, temporary workers, contractors and volunteers.
- All corporate records created at team level are stored on a shared team drive to enable relevant staff to have access to them as and when required.
- No corporate records are stored on staff personal drives or desk top computers.
- All electronic corporate records are saved in a shared drive to ensure all staff that require access are able to access what they need for their job role.
- records containing personal or sensitive data are stored in accordance with the data protection principles outlined in the college's Data Protection Policy.
- the college records classification scheme and standard file naming conventions are implemented to enable ease of access to information within the department.
- access to records is provided for all authorised users and access is tightly controlled to sensitive or highly confidential information.
- records required for business, accountability or cultural purposes are retained and remain usable for as long as they are needed.
- "vital" records are identified and copies stored securely off-site to enable business continuity.
- the college records retention schedule is implemented and managed for the functions for which they are responsible.
- records of long term or historical value are identified and preserved.
- other records are confidentially destroyed when they are no longer required in accordance with the records retention schedule.

4.2. All staff are responsible for ensuring that records created in the course of their duties are accurate and up to date.

4.3. The College Secretary is responsible for ensuring adequate records are created and maintained for all "Freedom of Information" (FOI) requests and all requests relating to the Environmental Information Regulations (EIR).

4.4. The college Data Controller is responsible for ensuring adequate records are created and maintained for all "Subject Access" requests.

4.5. The Information Development Manager is responsible for providing advice and guidance to staff with regard to record keeping, storage and destruction of documents, as well as maintenance and monitoring of the college wide records retention schedule.

The management of the college's archive records rests with the Information Development Manager who will ensure confidential destruction of records once the retention period has passed.

5. Supporting Documents

The following documents are available to support the implementation of the records management policy:

- Records Classification Scheme
- Records Retention Schedule
- File Archiving Procedure
- Access to Archived Records Procedure
- Guidance Note on Storage and Disposal of Documents
- Data Protection Policy & Associated Guidelines for Staff

6. Data Sharing

The sharing of personal data is covered by UK Data Protection Legislation and the EU General Data Protection Regulation (GDPR). Staff considering data sharing with a third party must first seek guidance from the college Data Controller at the earliest opportunity to discuss the purpose and nature of the proposed data sharing. In order to comply with legislation as well as manage and safeguard all personal data, a Data Sharing Agreement must be put in place between Inverness College UHI and the third party organisation. The legal basis for the sharing of personal data must be established and appropriate privacy notice(s) put in place. Where the legal basis for sharing is consent, consent must be obtained, prior to any data sharing taking place.

7. Access Arrangements

The college information audit identified at departmental level the records that require limited or controlled access. Departmental managers, Team Leaders/Co-ordinators will ensure that access and security arrangements are reviewed periodically and revised as necessary, especially during periods of staff turnover.

8. Responsibility for In-active Records

Departmental Managers, Team Leaders/Co-coordinators will ensure non-current (hard copy) records that must be retained for either legislative or external audit purposes are boxed up (in line with the college File Archiving Procedure) and stored within the central college archive. Additional guidance (if required) should be sought from the Information Development Manager.

When an electronic records management system is in place, electronic records will be removed from view when they are no longer current and retained within the electronic archive until the retention period has been reached.

9. Monitoring & Compliance

The college Information Development Manager will monitor compliance with the records retention schedule in relation to the processing of personal data. Electronic records management activity will be monitored through review of customised system reports (once the electronic records management system is in place) and work in conjunction with departmental records management contacts to ensure on-going compliance with this policy. Activity will be reported to the senior management team on a regular basis.

10. Implementation Details

Staff will be made aware of this policy via the normal consultation process associated with new policies. Training on the electronic records management system will involve reference to the records management policy and the associated supporting documents.

Each support department will have a nominated “super user” for the electronic records management system and this person holds additional responsibilities at team level for on-going records management duties. The “super users” will be supported (in a records management capacity) by the Information Development Manager.