University of Sunderland – Business Assurance

Records Management Policy

Policy Reference – Central Register _____	
Policy Reference – Faculty / Service _**IG06**_____	
Policy Owner	**Director – Business Assurance**
Date Policy Written	**March 2011**
Date Policy Last Updated	**October 2013**
Date to IG Group/Audit Committee	**December 2013**
Date for next Review	**March 2017**
Comments	

1. Introduction

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.

Records created by the institution to support its core functions and to comply with legal and regulatory obligations, must be handled effectively to contribute to the overall management of the University. This policy provides a framework for managing the University's records and introduces a series of Records Management related policies, procedures and guidance notes which have been drawn up in conjunction with the Lord Chancellor's Code of Practice on the Management of Records revised and reissued under s46 Freedom of Information Act 2000 and associated guidance from the Information Commissioner's office.

2. Purpose and Scope

This policy applies to all records created, received or maintained by staff of the University and Independent Contractors in the course of carrying out their work for the University.

The key objectives of this policy are to ensure:

- Authenticity of records

An authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have created or sent them, and to have been created or sent at the time purported.

- Integrity and availability of records

Information shall be available and delivered to the right person, at the time when it is needed.

The contents of a record should be trusted as a full and accurate representation of the activities or transactions to which they relate. The integrity refers to it being complete and unaltered. A record should be protected against unauthorised alteration. Any authorised annotation, addition or deletion to a record should be explicitly indicated and traceable.

- Confidentiality /Security of records

Access to records shall be confined to those with appropriate authority. Records must be securely maintained to prevent unauthorised access, alteration, damage or removal. They must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Where records are migrated across changes in technology, the University must ensure that the evidence preserved remains authentic and accurate and is in a readable format.

3. Definitions:-

3.1. Record

The International Standards Organisation (ISO) defines records as "recorded information, in any form, created or received and maintained by the organisation in the transaction of its business or conduct of affairs and kept as evidence of such activity". These include:

- corporate administrative records (paper or electronic)

- photographs, CCTV and scanned images
- microform (fiche / film)
- audio and video tapes, DVDs, CD ROMs, cassettes
- databases, spreadsheets
- maps, drawings and plans
- emails and if applicable their attachments
- text messages – received and sent
- voicemail recordings

3.2. Records Management

Records management is a discipline which uses an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the organisation and preserving an appropriate historical record.

4. Responsibilities

The Executive member with overall responsibility for this policy is the Deputy Vice Chancellor and Deputy Chief Executive. S/he is responsible for deciding on the outcome of internal reviews of Freedom of Information requests and EIR requests.

The Assistant Director of Business Assurance, who performs the role of the University's Senior Information Risk Owner (SIRO)is responsible for:

- Ensuring that an overall culture exists that values and protects information within the organisation
- Owning the organisation's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used
- Owning the organisation's information incident management framework

The Assurance Manager (Business Assurance - Information Governance), responsible to the Assistant Director for Business Assurance ,is responsible for drawing up information governance and records management policy, process and guidance and ensuring compliance with this policy.

The University Deans of Faculty and Directors of Support Services have responsibility for ensuring compliance with the University's Information Governance policies and ensuring any issues of non-compliance are addressed. They have responsibility for ensuring that an appropriate member of staff, in each Faculty and Service, takes on the role of "Information Champion".

The Information Governance Group is responsible for recommending policy direction on information governance to the Executive and monitoring that agreed policies are followed.

Information Champions are accountable to their Dean of Faculty/Director of Service and have a responsibility to monitor information governance compliance and awareness and be the primary point of contact and source of information and support within the Faculty/Service. The Information Champions Group will report to the Information Governance Group.

Individual employees and contractors have responsibility for ensuring that they comply with this policy and any related policies and guidance. Staff should attend training and awareness se ssions provided by the University. Employees also have a duty to report any incidents or 'near misses' in relation to information governance.

5. Policy Details

The University is committed to creating, keeping and managing its records in a manner that accurately documents its principal activities and that meets its statutory obligations.

All records created or received by University staff in the course of their employment are the property of the University and subject to its control. Employees leaving the University or changing posts within it are required to leave all records for their successors.

The key components of records management are:

- record creation
- record keeping
- record maintenance (including tracking of record movements and access)
- disclosure and transfer
- appraisal, archiving and disposal or destruction.

5.1. Records Creation

Records will be created and information captured in such a way that it is:

- readable; records have little value if they are not readable therefore consideration should be given to the format in which a records are created
- authored; the name and title of the author to be included in the record at the point of creation
- countersigned or approved where professional authority is required
- date and time stamped
- contemporaneous and timely
- version controlled
- validated
- protectively marked to identify the level of confidentiality that the record requires. The Information Classification Policy should be consulted.

5.2. Record Keeping

Key to implementing and maintaining an effective records management service is the knowledge of:-

- What records are held?
- Where they are stored?
- Who manages them?
- In what format?

An information survey will be carried out to fulfil these requirements and to provide data for developing records appraisal and disposal policies and procedures.

The record keeping system, whether paper or electronic, should include a documented set of rules for referencing, titling, indexing and, the protective marking of records. This will enable the efficient retrieval of information when it is needed and help to maintain security and confidentiality. The Information Classification Policy should be referred to.

Additionally, a business categorisation scheme may be implemented which will also facilitate the application of retention periods, in line with the Records Archive and Retention policy.

Staff should be aware of the University's obligations to provide information to respond to Freedom of Information requests, including any University information held in private accounts or on privately owned IT equipment. It is therefore in the interests of both the

University and staff that University information should be stored in University provided storage.

It is also important to note that records and documentation created in the course of research, whether internally or externally-funded, are also subject to contractual record-keeping requirements. Advice should be sought when storing information of records classified 'Confidential', 'Sensitive' or 'Secret' as determined by the Information Classification policy. Suitable contacts are listed on the policy cover sheet.

5.3. Records Maintenance

Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. Tracking mechanisms for paper records will record the following as a minimum:

- the file name and/or number
- a description of the file content
- the person, unit or department to whom the record is being sent
- the date of transfer

Storage accommodation for current records should prevent damage to the records and ensure a safe working environment for staff.

The record will reliably and accurately represent the information that was actually used in, or created at the time of initial development, and demonstrate its integrity and authenticity.

Digital records will need to be maintained to ensure that the information contained within them is readable given the changes in the format of records over time.

It should also be noted the classification of records can change over time. Therefore any records maintenance procedures should include the need to review the classification in line with the Information Classification policy.

Access

Records must be made secure from unauthorised or inadvertent alteration or erasure, ensuring that access and disclosure are properly controlled and audit trails will track all use and changes. This must be undertaken in accordance with Information Governance policies, particularly the Information Classification policy and Information Security policy.

Emails as Records

The primary function of the Microsoft Outlook email system is for communication rather than a storage system for electronic records. Staff will be responsible for ensuring that emails or attachments that constitute a 'record' are managed in accordance with this policy, and that email records are saved in secure locations outside of the email system and are easily accessible when required.

5.4. Disclosure and transfer

A range of statutory and regulatory obligations, such as those contained within the Data Protection Act, are placed upon an organisation when disclosing or transferring information to a third party.

When the University enters into a partnership, protocols should be established with the partner organisation covering the storage and retrieval of information, the information to be retained

and by whom, the level of security required, who has access to the records and the disposal arrangements.

5.5. Appraisal, archiving and disposal or destruction

In line with the requirements of the Data Protection Act, records will not be held for longer than necessary. The University has adopted the JISC retention model and where this does not satisfy the business requirements, additional retention schedules will be developed at a service level.

The organisation will ensure that records are disposed of appropriately using consistent and documented retention and disposal procedures. Records requiring longer-term or permanent preservation will be archived. The University's Records Archive and Retention policy and associated procedures should be referred to.

5.6. Incidents Involving Records

Any incidents involving the inappropriate use, loss, alteration, inappropriate storage or accidental or malicious disclosure of records will be managed in accordance with the University's Incident Response plan and other related Information Governance policies as listed in the Appendix A of the Overarching Information Governance Policy.

6. Relationship with other University policies

This policy should be read in conjunction with the policies listed in Appendix A of the Overarching Information Governance Policy.