

Records Management Policy

Introduction

This Policy forms part of a suite of policies and procedures that support a Data Protection Framework relevant to the maintenance of accreditation to BS10012:2017 – Specification for a Personal Information Management System (PIMS)

A record is defined in the Records Management British Standard ISO15489 as “Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business”. All records created and held by the University, both paper and digital, (including email and information held in databases) are subject to this policy.

Records are an important asset to the University and they require appropriate management for effective and efficient administration, for the discharge of University responsibilities and business, and for compliance with legislative requirements. Good management of records also helps staff in the performance of their duties by improving access to and organisation of relevant records, removing out of date or superseded records from University systems and reducing duplication of documents and data. There are also several sets of legislation which impact on the way in which the University manages information. Non-compliance with this legislation carries financial and reputational penalties.

Purpose

University records are defined as those documents or data sets which arise from or facilitate the business carried out by the University and which provide evidence of its transactions or activities. This Policy aims to ensure that the University creates, maintains, retains and properly disposes of those records which it requires for the conduct of its business and that they are managed in a manner commensurate with legal obligations and information requirements. The University acknowledges the legislative environment within which it operates, particularly in the context of this Policy, those pieces of legislation, related codes of practice and standards listed in the control

box below. These all have implications for the way in which public authorities are expected to keep records and apply records management standards.

This will be achieved through the implementation of controls and responsibilities including measures to ensure:

- Legislative compliance - compliance with record keeping provisions in current legislation such as the Freedom of Information Act, the Data Protection Act and the Environmental Information Regulations.
- Information lifecycle management – records must be kept for an appropriate length of time and in an appropriate manner. They must be disposed of at the end of their lifecycle in accordance with policies, procedures and best practice and in accordance with the University’s Records Retention schedule.
- Confidentiality – University records must be protected from unauthorised access. • integrity – the accuracy and completeness of University records must be safeguarded and unauthorised amendment or destruction prevented.
- Availability – University records must be available to authorised users in line with business and funding body requirements.
- Efficiency – University records must be available to authorised users in a form that ensures efficiency and ease of use.
- Authentication – the identity of the persons accessing highly restricted and critical systems which permit the creation, amendment or deletion of University records must be recorded and verifiable
- Semi-current manual records (records which are not in regular use, but which have not yet reached their disposal date) will be managed, where appropriate, by the relevant College or Service in conjunction with Library & Learning Services.

Scope

This Policy applies to:

- All University records;
- Research records, whether internally or externally funded are included, as are records sent or received through the email system;

- All members of staff, as well as individuals conducting work at or for the University and/or its subsidiaries, who have access to University information (“staff”). This includes temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the University and suppliers (this list is not intended to be exhaustive); and
- All locations from which University information is accessed including off-campus locations.

Responsibilities and Compliance Framework

The University has a corporate responsibility to maintain its records and records management systems in accordance with the regulatory environment. This responsibility therefore extends to all staff who work with University records. Email must not be used for storing University records. Any email that is important and needs to be retained must be stored elsewhere in an appropriate filing system relevant to their confidentiality, criticality or data classification. Pro-Vice Chancellors, Heads of Schools or Colleges, Directors or equivalent are responsible for ensuring that records management within their areas is carried out in line with this Policy and established procedures. To assist with this, the University will be identifying Data Liaison Officers (DLO’s) across all organisational units, areas and Schools. DLO’s will be responsible for helping to ensure that records are managed appropriately within their areas. The Information Assurance Office is responsible for providing policies, procedures, guidance and advice in support of this Policy and wider data protection, for training staff where necessary for demonstrating ongoing regulatory compliance with laws associated with the management of information including Data Protection, Freedom of Information and e-Privacy.

Monitoring Compliance

The PIMS and its associated policies are subject to internal monitoring and auditing throughout the University, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. The University will also undertake appropriate benchmarking and this policy will be audited by external bodies. Reports on the matters related to all policies within the PIMS will be provided to the Vice Chancellors Group.

Version Control

Document Version Number	1.0
Document Owner	Data Protection Officer – Vice Chancellors Group
Document Approved By	Vice Chancellors Group
Approval Date	18th March 2018
Review Date	This policy may be amended to reflect changes in the Data Protection Bill that occur when the Bill receives Royal Assent prior to becoming the Data Protection Act 2018.