
# Records Management Policy

**Contents**



## 1. Overall Commitment

1. The University recognises that good records management is necessary to support:-
   - its Vision and Strategic Plan
   - the functions that it undertakes to support teaching and learning, research and administration
2. It also enables:-
   - improved transparency and accountability
   - effective and informed policy formation and decision-making;
   - the management of business risks and continuity in the event of disaster or events
   - the protection of rights and obligations for the University and individuals that work for and with it
   - protection and support in litigation
   - compliance with legislation and regulations
   - improved ability to demonstrate corporate responsibility, including meeting sustainability goals

- reduction of costs through greater business efficiency
- protection of intellectual property
- evidence-based research and development activities
- the protection of corporate, personal and collective memory

3. This document sets out the policy through which effective management can be achieved and audited. It forms part of a suite of policies, standards and associated procedures and guidance designed to improve the management of information within the University.
4. The University aims to create and maintain authentic, reliable and useable records that support business functions and activities for as long as required.
5. Records should be maintained throughout their lifecycle with appropriate security arrangements, organisational arrangements and metadata to ensure their authenticity, reliability, integrity and useability. See appendix one for a full definition of a record's characteristics.
6. The University is committed to understanding and documenting the following:-
    - What records are held
    - Where are they held
    - How are they held
    - Why they are held
    - What business activities they support
    - Who has access to them
    - Who manages them
    - How long should they be retained for

## 2. What does the Policy apply to?

1. The policy applies to records held by the University, within University record keeping systems, as well as those stored, managed or hosted on behalf of the University within third party systems or facilities. Records are defined as *information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.* For a full list of definitions see appendix one.
2. It relates to content created by the functions, activities and transactions carried out by, or on behalf of, the University.
3. The main functions and activities include, but are not limited to, teaching and learning, research, knowledge transfer and enterprise, academic administration, corporate management, corporate resources, corporate relations, related companies, commercial services, corporate services, student services and business units. A wider description of these functions and activities is available within the JISC Business Classification Scheme that the University has adopted as a template for the functions and activities it undertakes.
4. Records can be created and held in any form of media, and this policy applies to records of any format that have been captured into a record keeping system.

## 3. Who does the Policy apply to?

1. The policy applies to all staff employed by the University of Sheffield. This includes all permanent and temporary employees, contractors, consultants and secondees.
2. The Policy also applies to third parties that have a formal contractual relationship to store, manage or host records on behalf of the University. In particular the requirements of third parties that process personal data on behalf of the University should adhere to the requirements set out under Article 30 of the GDPR to document a Record of Processing Activity.

## 4. Governance and responsibilities framework

1. The University has developed an information governance framework setting out roles, responsibilities and accountabilities. The main roles, responsibilities and accountabilities are set out below.
2. The University Executive Board is responsible and accountable for approving the strategic direction and policy framework for information management developed by its Information Management and Security Group (IM&SG).
3. IM&SG has been delegated responsibility and accountability for recommending policy, monitoring and reporting on compliance and reporting risk. IM&SG will provide the strategic direction and oversight required to ensure a consistent framework of policies and procedures encompassing the storage, retention, structure, use, protection and gaining value from information assets in relation to the strategy and purposes of the organisation while meeting our regulatory and statutory requirements.
4. The Executive Director of Academic Services, Executive Director of Corporate Services and the Chief Financial Officer are accountable officers for the management and use of information systems, data management and processing at the University and for fostering a culture for using and protecting data, that information is accurate and its value is realised, information is secured and legislation is complied with.
5. The University Secretary is responsible for the general oversight of compliance and risk in relation to information governance.
6. Senior Information Asset Owners (SIAOs) have responsibility for a process and / or system. They are typically Directors of Professional Services. They are must know what information systems and assets they are responsible for, what information is held and shared by their systems, the linkages between systems, and who has access to the information within the systems.
7. SIAOs will also be responsible for ensuring that the Policy requirements for record keeping systems (section 5) and retention and disposal (section 8) are appropriately implemented and documented.
8. Faculties and Departments are responsible for their own information processing at various levels and requirements.
9. Faculty Vice Presidents and Heads of Department have responsibility for the implementation of University information governance policies and procedures in their Departments and Services.
10. The University Records Manager is responsible and accountable for setting the records management framework, providing guidance and advice to departments on all aspects of record keeping and promoting good information management practices within the University.
11. The University Secretary's Office, via the University Records Manager, is responsible for overseeing implementation and monitoring of, and compliance with the Policy, and for reporting appropriately to the IM&SG.
12. Information Champions are appointed by Heads of Department to work on their behalf to ensure that policies are followed, mandatory training is completed, information asset registers are maintained and act as a local point of contact for incident reporting.
13. Information users, those working day to day with information, are responsible for information they are using and must follow relevant policies, procedures and processes.
14. Departments are expected to adhere to policies and procedures set out by the IM&SG, and to ensure that appropriate capacity and resources are set aside to undertake activities and tasks set by it.

## 5. Record keeping systems

1. Almost all business applications will generate data that will need to serve as evidence of business activity for future reference and therefore will need the ability to create, store and manage records. These applications are hereafter called record keeping systems.
2. Record keeping systems must be reliable, secure, comprehensive, compliant and systematic. See appendix two for a fuller definition of these characteristics.
3. Record keeping systems must be able to support the high level functional requirements for applications that manage University business processes. These are set out in detail in appendix two. This must be appropriately documented.
4. It is not permitted to develop record keeping systems that bypass official corporate systems whose use is mandated by the University.
5. Localised record keeping systems are only permitted if they support a required function or activity that is not currently operationally supported by central systems, and is appropriately authorised.
6. When procuring or refreshing a record keeping system there must be accompanying documentation of the ability of the system to support high level functional requirements supporting University business processes (see appendix two).
7. All records created or received by staff during the course of University business should be captured into an appropriate record keeping system. Records should be captured as soon as possible after creation so that they are readily available to support the University's business activities.
8. Record keeping systems may be designed specifically to manage records, or may be systems designed for other business processes that are adapted so that they also support the creation, capture and management of records.
9. Record keeping systems utilised by departments must be recorded in departmental Information Asset Registers. An Asset Register will record:-
    - A description of the record keeping system
    - The business function that it supports
    - The type of information that it holds
    - Retention and disposal requirements to be applied
    - Any sharing of the data with third parties
    - Security arrangements
    - Ownership information
    - Location of the asset
    - A Classification grading
10. The Asset Registers should be maintained and reviewed at regular intervals to ensure they contain up to date information of information assets.

## 6. Storage of records

1. The storage of records must be governed by appropriate access controls that are documented and take account of information security protocols.
2. Records and record keeping systems must have in place protection to the level required by the nature, contents and value of the information in them.
3. Storage conditions should be designed to protect records from unauthorised access, loss or destruction and from theft and disaster.
4. Storage of records must align to the requirements of the University Classification Scheme and Handling guidance.
5. Records should be stored on media and in formats that ensure they are accessible and interpretable for as long as they are required.
6. Access to record keeping systems and to records should be applied where necessary and documented within the Information Asset Register. Access to third parties outside of the University must be appropriately documented.

## 7. Classification and Handling of records

1. The University has developed a Classification and Handling Scheme for information. It can be downloaded from the University Secretary's Office, Records Management Policy and Guidance web page.
2. Records and record keeping systems must align to the requirements of the University Classification Scheme and Handling guidance.
3. Any record keeping system should be capable of holding and providing access to records in a manner that is commensurate with the Classification applied.

## 8. Retention and Disposal

1. The University has created and maintains a Records Retention Schedule. It can be downloaded from the University Secretary's Office, Records Management Policy and Guidance web page.
2. The University Records Retention Schedule (RRS) sets out retention and disposal timescales for business processes and activities that create records.
3. The requirements set out in the RRS should be applied to record keeping systems that hold the relevant records.
4. If it is not possible to apply the requirements of the RRS, steps should be taken to document this and to apply such requirements when systems are refreshed or renewed.
5. Disposal activities should be undertaken by authorised members of staff and in as secure a manner as required by the Classification of the material such that it is protected from unauthorised access.
6. Disposal activities should be appropriately documented and retained to provide an auditable trail.
7. The RRS is updated as appropriate and should reflect retention periods in line with statutory, regulatory and administrative requirements.
8. The RRS is reviewed and agreed by those departments who are deemed to be the senior information asset owners.
9. The RRS will also identify any records worthy of permanent preservation.

## 9. Long term retention

1. Records or data should be retained and maintained in an authentic state for as long as they continue to be required, regardless of any technology change that may occur.
2. Systems that create or capture records or data must do so with due regard to long term preservation requirements and other requirements set out in this Policy, specifically those required to ensure the characteristics of records set out in appendix one.
3. The University may retain certain data within central systems or records on a permanent basis. This may form part of the corporate archive of the University that may be open to researchers, or may be retained permanently within corporate systems in order to satisfy continuing statutory, regulatory or administrative requirements.
4. The University retention and disposal schedule will highlight any records worthy of permanent preservation, or records that may be reviewed with a view to permanent preservation.
5. Records retained permanently will be consistent with the University's archive collecting policy.
6. Records retained permanently are exempt from certain data protection provisions and will rely on appropriate exemptions set out within data protection legislation.

## 10. Relationship with other Information Management policies and procedures

1. The Records Management Policy forms part of a suite of policies and guidance on the management of information at the University. This includes the University's Data Protection Policy and Information Security Policy.
2. There is a range of documentation that departments should use in order to manage their records appropriately. This includes documentation on retention and disposal, Information Asset Registers and Information Classification and Handling protocols.
3. Nothing within this policy should be inconsistent with other policy guidance regarding the management of information.
4. Good records management supports and improves information security and data protection compliance at the University.

## 11. Legislation, regulations and standards

1. The University acknowledges that the management of records should take into account appropriate legislation, regulations and standards. These inform particular record keeping activities and frameworks departments should adhere to when undertaking their functions and activities.
2. Particular statutory requirements such as The General Data Protection Regulations and Health and Safety legislation will determine specific retention requirements.
3. Departments should ensure that where there may be statutory, regulatory or other relevant codes of practice setting out record keeping requirements these should be incorporated into local policies, processes and procedures as well as the University RRS. This will include, but not be limited to, functional areas such as Health and Safety, Safeguarding and Financial Management as well as particular areas of clinical or health related research.
4. The University will seek to incorporate guidance set out in ISO Standard documentation relating to record management into systems and processes. These are set out in appendix one.
5. The Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000 (pub. 2009) also sets out expectations for the appropriate management of records.

## 12. Monitoring, Implementation and Compliance

1. The University will put in place a monitoring, implementation and compliance framework to ensure that the Policy is adhered to and that records management practices improve and mature.
2. The monitoring, implementation and compliance framework will reflect the University's information management needs and arrangements and the risks that non-compliance with the Policy would present.
3. The framework will allow for a reporting of maturity and assurance relating to records management activities, allowing it to assess itself against the commitments set out above.
4. This framework will be overseen by the IM&SG who will report to UEB.
5. Departments will be expected to put in place the means by which performance can be assessed. This will consist of local policies, processes and procedures, as well as appropriate resources, responsibilities and accountabilities for record keeping and the maintenance of activities.
6. Those who have responsibilities and accountabilities for records management will be expected to oversee their areas and to provide support and assistance in implementing the requirements of this Policy.

## 13. Updating the Policy

1. This Policy is owned and approved by the IM&SG.
2. The Policy's Change Manager is the University Records Manager.
3. The policy will be subject to a formal review by the Records Manager every two years, but may be amended at any time between formal reviews in light of any statutory or regulatory guidance that needs to be taken account of.
4. Departments may also request variations or exemptions to certain elements of the Policy in consultation with the University Records Manager, based upon legitimate business requirements.

**Records Management Policy, v2.0**

**Information Management and Security Group**

**October 2020**

# Appendix one - definitions and documentation

## Definitions

## ISO 15489-1:2016 Information and documentation - records management

### Records
Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

### Records Management
The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of an information about business activities and transactions in the form of records

### Records system
Information system which captures, manages and provides access to records over time.

### Information Asset
An information asset is defined as “a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.
Information assets have recognisable and manageable value, risk, content and lifecycles.

### Information Asset Register
A register that records information assets being used.

---

## ISO 30300:2020 Management systems for records

### Characteristics of reliable records
Information, documents or data that are to be retained in a record keeping system should possess the following characteristics to ensure that they provide authoritative evidence of transactions to support activities and functions.

### Authenticity
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.

### Reliability
The contents of a record should be trusted as a full and accurate representation of the activities or transactions to which they relate. Records must be sufficient in content, context and structure to reconstruct the relevant activities and transactions that produced it.

### Integrity
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.

### Useability
A useable record is one that can be located, retrieved, presented and interpreted. A useable record should be connected to the business process or transaction that produced it.

## Characteristics of reliable records systems
Business applications should have specific characteristics that support the delivery of records possessing characteristics listed above.

### Reliable
Reliable records systems routinely capture all records within the scope of the business activity they cover. They organise the records in a way that reflects the business processes. They protect records from unauthorised alteration or disposition. They routinely function as the primary source of information regarding actions documented in the records.

### Secure
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.

### Compliant
Compliant records systems are systems which are managed to meet all requirements arising from current business and stakeholder expectations and the regulatory environment in which the University operates. Systems can be assessed for their compliance with respect to these requirements as part of the maintenance and improvement processes and they ensure organisational accountability, good governance and risk management.

### Comprehensive
Comprehensive records systems should be capable of managing all required records of the range of business activities to which they relate

### Systematic
Records systems should be designed to automate records processes as much as is practicable through their design and routine application of authorised policies and procedures.

---

## Applicable International Organisation for Standardisation (ISO) documentation

- Information and Documentation – Records Management. ISO 15489-1:2016
- Management systems for records - ISO 30300 / 30301  30302
- Records Management in enterprise architecture - PD ISO / TR 21965:2019
- Evidential weight and legal admissibility of electronic information - see BS ISO 10008:2020
- Risk Assessment for records processes and systems - PD ISO / TR 18128:2014
- Work Process analysis for records - PD ISO / TR 26122:2008
- Data protection. Specification for a personal information management system - ISO 10012: 2017+A1:2018

# Appendix two
# Model high-level functional requirements for applications that manage digital records

**Introduction**

Organisations deploy software applications to automate business activities and transactions. The digital information generated may serve as the only evidence or record of the process or transaction, despite the application not being designed specifically for the purpose of managing records.

Because of the dynamic and manipulable nature of data in applications and systems, the capture of records and the ongoing management of their fixity, authenticity, reliability, integrity and useability can be challenging.

It is assumed that almost all business applications will generate data that will need to serve as evidence of business activity for future reference. The purpose of this document is to assist the developers and implementers of those applications to identify and deploy functional requirements that will help ensure that the data generated and held in such applications can serve as adequate records of business activity.

Many business applications generate and store data that may be subject to constant updating (dynamic), able to be transformed (manipulable) and only contain current data (non-redundant). These are all entirely legitimate but organisations must also use data to serve as reliable evidence of business activity. If this is the case then the records created need to be fixed and inviolable. That is systems and processes need to be able to guarantee the reliability and authenticity of the records as evidence of past business activity.

**Overarching attributes and characteristics**

Attributes of records held within business applications

- Authenticity
- Reliability
- Integrity
- Useability

Characteristics of business applications that manage records

- Secure
- Compliant
- Comprehensive

- Systematic

**Determining the need for evidence of events, transactions and decisions in business applications**

Not all information contained in a business application will necessarily be required to be recorded as evidence. Before reviewing, designing, building or procuring business applications, it is necessary to determine the organisation's needs for records in order to develop and deploy appropriate strategies and technologies. (Further details can be provided for each step).

Step 1 - Identify requirements for evidence of business using functional analysis
Step 2 - Analyse the work process
Step 3 - Identify the information that records this evidence
Step 4 - Identify linkages and dependencies
Step 5 - Reflect records requirements in functional requirements for software and determine implementation options

Many processes will extend beyond a single business application. Necessary linkages to other applications or related information should be considered before strategies are developed to manage records in the business application. A key dependency is how long records (data) need to be kept. This is often based on a period of time that is in accordance with legislative, regulatory and business requirements. This is documented in a retention and disposal schedule.

**Key outcome areas**

1. **Records capture and classification.** Software applications that enable business activities and transactions should be able to capture and / or import / ingest evidence of those activities. This involves identifying sets of digital information to serve as records. Records have to be linked to their business context using metadata.
2. **Records retention and disposition.** Records shall be kept and remain accessible for as long as required for legislative, regulatory or business needs. Records should be retained and disposed of in a managed, systematic and auditable way.
3. **Records integrity and maintenance.** Business applications should be able to register any interactions with or changes to the records.
4. **Records discovery, use and sharing.** Business applications should enable searching, retrieval, rendering, use, sharing and redaction of records for authorised users. They should also support interoperability across platforms and domains over time.

**Model high level functional requirements for applications that manage digital records**

1. Capture and classification
    1. Records creation, capture and import
    2. Records metadata capture
    3. Records classification
    4. Managing business classification schemes
2. Retention and Disposal
    1. Records retention, review, transfer and destruction
    2. Records migration and export
3. Integrity and Management

    1. Records authentication and security
    2. Storage, reporting and metadata management
4. Discovery, use and sharing
    1. Search, retrieval, presentation, use and interoperability
    2. Access restrictions and permissions
    3. Duplication, extraction and redaction

**Obligation levels**

| | |
|---|---|
| **Shall** | Requirements that use 'shall' are a requirement for compliance with the specification |
| **Should** | Requirements that use 'should' may be ignored if a valid reason exists, but the full implications of ignoring the requirement should be understood and carefully considered and documented before choosing a different course |
| **May** | Requirements that use 'may' are optional |

| **1 Capture and classification** | **Obligation** |
|---|---|
| **1.1 Records creation, capture and import** | |
| The business application shall, either alone or in conjunction with other applications:<br>Enable the capture of records and any associated records metadata<br>Where individual applications cannot provide the business capability other components must provide the capability to ingest records and / or associated metadata.<br>Where the application creates or receives records generated by electronic messaging systems, capture attachments and embedded objects together with the digital messages as either linked records or as a single compound record.<br>Enable the business application to import digital records and associated metadata directly from an external business application, either in bulk or individually, ensuring the integrity of the content and structure of the records | Shall |
| Not limit the number of records that can be captured and retained by the application.<br>Support capture of the range of file formats routinely used by the business in their native formats | Should |
| **1.2 Records metadata capture** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Enable the capture and maintenance of metadata for records at any time during the record's existence, in accordance with one or more pre-determined metadata schema(s).<br>Be able to assign and persistently link unique identifiers to each record and records aggregation.<br>Support the ability to automatically detect and capture pre-existing metadata for records from business processes and associated information systems.<br>Be able to capture metadata entered manually by a user. | Shall |
| The business application should, either alone or in conjunction with other applications:-<br>Support the ability to validate metadata values against pre-determined schemes and / or syntactical standards.<br>Support common business formats (eg XML) or combinations of formats for metadata / properties. | Should |

| | |
|---|---|
| Allow authorised users to add annotations or notes to records as linked metadata in accordance with business rules and policies. | |
| The business application may, either alone or in conjunction with other applications:-<br>Be able to associate records at individual object and / or aggregation level to their business context.<br>Support documentation of changes to business context over time, retaining the ability to link business context accurately over time | May |
| **1.3 Records classification** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Be able to associate records at individual object and / or aggregation level to their business context.<br>Support documentation of changes to business context over time, retaining the ability to link business context accurately over time | Shall |
| **1.4 Managing business classification schemes** | |
| The business application may, either alone or in conjunction with applications:-<br>Manage and maintain an approved business classification scheme | May |
| **2. Retention and Disposition** | **Obligation** |
| **2.1 Records retention, review, transfer and destruction** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Be able to allocate an appropriate retention and disposition period in the application.<br>Retain key metadata including metadata documenting disposition authorisation.<br>Store the status of the record as 'deleted' or 'transferred to x' from the date of the disposition.<br>Have the ability to stop the disposition process.<br>Report on disposition status and activity when records disposition is carried out within the application. | Shall |
| Automatically flag records as eligible for disposition and dispose of them once their retention periods have expired and, if required by a disposition authority, the records have been reviewed by an authorised agent / user.<br>Restrict the operation of the disposition process to a business application administrator.<br>Support a range of disposition triggers based on active metadata. For example:-<br>• date of record creation<br>• date of last retrieval of a record<br>• opening or closing date of an aggregation of records<br>• date of last review of a record or aggregation of records<br>Support the capability to archive records and / or transfer records of continuing value together with their metadata to an authorised third-party archiving service.<br>Allow for the destruction of records to result in the complete obliteration or inaccessibility of the contents of all records as authorised, and that they cannot be restored through operating system features or specialist data recovery techniques | Should |
| **2.2 Records migration and export** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Be able to migrate / export records and associated metadata, and where applicable aggregations of records to:-<br>• a more appropriate or up to date file format for the records<br>• another business application within the organisation<br>• a replacement business application when the source application is due for decommissioning | Shall |

| | |
|---|---|
| • a system in a different organisation<br>Ensure that any export / migration action is able to include:-<br>• all records, and where applicable aggregations of records<br>• metadata associated with exported records and aggregations of records<br>• event history metadata associated with exported records<br>Be able to migrate / export digital records and where applicable aggregations of records such that:-<br>• the content and structure of records and aggregations of records are not degraded<br>• associations are retained between exported records and their associated metadata<br>Relationships are maintained between exported components of a record, between exported records, and where applicable aggregations of records, so that their structural links can be re-built in the receiving application<br>Be able to test to ensure that the integrity of the records and key metadata is not degraded below the minimum standards set by the business and / or jurisdiction<br>Allow records to be exported / migrated more than once | |
| Be able to implement the destruction of source records where they have been superseded by migrated / exported records in the new application.<br>Be able to access underlying data tables and content of the application following its decommissioning, via a viewer or using virtualisation technology, where inactive / closed records are not to be migrated.<br>Support content access control for records applied at record level and persistence of that control when content is exported / transmitted / migrated from the host application | Should |
| **3 Integrity and Management** | **Obligation** |
| **3.1 Records and authentication and security** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Ensure that the content of records can be fixed or protected from unauthorised alteration.<br>Enable controls over the alteration or editing of metadata in accordance with business rules stipulated by the organisation.<br>Be able to generate checksums, hashes or other mechanisms to support integrity checking at points in time.<br>Routinely authenticate any user before allowing access.<br>Automatically record and show the details of all authentication and security processes | Shall |
| Be able to capture and persistently store metadata that documents the use of digital signatures (date, time and validation) with the record.<br>Capture any other confirmation details for digital signatures in such a way that they can be retrieved with the record, but without compromising the integrity of a private key.<br>Allow electronic signatures to be added to content via workflow functionality, maintaining a record of the process.<br>Support the secure transmission of records, including the encryption of records for secure transmission where appropriate.<br>Enable the conversion of records into more suitable file formats to support ongoing retention and use. | Should |
| **3.2 Storage, reporting and metadata management** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Ensure that the records and associated metadata controlled by the application are persistently and securely stored and that they remain accessible and retrievable over time for their minimum retention periods to authorised users.<br>Be able to produce reports on records capture, usage and disposition.<br>Be able to report the actions carried out on records, either by the application itself or by authorised users and administrators | Shall |
| Be able to manage and / or link to approved metadata profiles or schemas over time in ways | Should |

| | |
|---|---|
| that support the automated capture and maintenance of validated metadata values for records and records aggregations | |
| **4 Discovery, use and sharing** | **Obligation** |
| **4.1 Search, retrieval, presentation, use and interoperability** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Provide users with tools for searching and retrieving records and metadata<br>Extract and render records in a useable format<br>Be able to integrate and interoperate with other management systems which have appropriate functionality where the business application is itself unable to undertake records functions | Shall |
| Allow users to define a workspace to allow multiple users to work together on a project<br>Support users to access records and records aggregations from mobile devices<br>Allow users to configure the application for personalised records views, searches or presentation services<br>Allow for collaboration with external third parties and for the sharing of records and / or metadata with external platforms, networks, services and collaborative workspaces<br>Be able to make approved data stored within the application available for harvesting by external services and applications as linked open data via application protocol interface using protocols such as OAI-PMH or CMIS | May |
| **4.2 Access restrictions and permissions** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Apply security and access restrictions ensuring that only authorised users can access records appropriate to their access rights<br>Apply security and access protocols to protect the content of of records and their metadata from unauthorised access, alteration or destruction<br>Create and maintain access, usage and security metadata, generating secure event logs for each specific record / record aggregation documenting access to and use of records | Shall |
| **4.3 Duplication, extraction and redaction** | |
| The business application shall, either alone or in conjunction with other applications:-<br>Support mechanisms to enable the authorised duplication of records or extracts of records for use either within the application itself or in other applications and / or organisations, in accordance with pre-determined business rules | Shall |
| Allow the creation of an extract from a record, whereby sensitive information is removed or hidden from view in the extract, while the originating record remains intact, ensuring metadata documenting the extraction action is generated and captured | May |
| | |

| | |
|---|---|
| **Date** | October 2020 |
| **Author** | Information Management & Security Group |
| **Owner** | University Information Management and Security Group |
| **Change Manager** | University Records Manager, The University Secretary's Office |
| **Purpose of document** | To have in place a policy for the management of records at the University of Sheffield |
| **Review cycle** | 2 years – Reviewed August 2020. Next review October 2022 |
| **Amendments** | 9/9/2021. URLs removed in 7.1 and 8.1. Reference made to obsolete URLs. Information Classification Scheme and Records Retention Schedule on University Secretary's Office Records Management Policy and Guidance pages. |