



Records Management Policy

Publication:	External (public)
Date approved:	19 February 2026
Approving body:	Senior Information Risk Owner (SIRO)
Date of next review:	January 2028
Review frequency:	Every 2 years
Policy/Regulation Owner:	James Bentley – <i>Associate Director for Information Compliance and Data Protection Officer</i>

1. Overview and Purpose

1.1 The purpose of this Policy is to expand upon the Information Risk Management Policy, by establishing University requirements in relation to Records Management. Records Management is the systemic and efficient control of the creation, receipt, maintenance, use, and disposal of records.

1.2 The University must create, hold, and eventually dispose of records that evidence its activities. These records are created and held throughout the University and constitute an essential legal and operational asset.

1.3 We recognise the importance and value of our records. Effective records management is necessary to support the University's core functions and makes a significant contribution to the management of the institution.

1.4 Records management enables the University to:

1.4.1 meet legislative and regulatory requirements

1.4.2 defend our interests in litigation and its legal rights more generally

1.4.3 undertake and document effective and informed policy formation and decision-making

1.4.4 recognise and manage business risks

1.4.5 evidence research, teaching, and learning activities and accomplishments

1.4.6 manage operations in an effective, efficient and evidence-based manner

1.4.7 preserve the collective memory and identity of the University

1.4.8 provide continuity in the event of a disaster

1.5 Any queries about this policy should be directed to the University's Information Compliance Team at records.management@uea.ac.uk

2. Scope

2.1 This Policy applies to all University employees, and those working on our behalf, in relation to all records, regardless of format, that are created, received or maintained by the University

in the course of carrying out its functions including research, whether internally or externally funded.

2.2 Adherence to approved policy and regulations is fundamental to the effective operation of the university. This policy has been developed in alignment with sector best practice to promote consistency, accountability, and compliance with relevant standards. Observing the policy ensures that decisions and actions are informed, equitable, and aligned with institutional values.

2.3 This Policy is supported by further documents outlined in Section 6.

3. Definitions

Term	Definition
Archive	Records which are permanently preserved because they are considered to have enduring public, research, historical, informational, evidential or legal value.
Business classification	A label attributed to a data, information, or document establishing how it is categorised into an organisational function in line with the Business Classification Scheme
Business classification scheme	A documented systematic identification and arrangement of business activities that allows data, information and documents to be linked to the business context of their creation.
Data	Facts, observations, statistics, characters, symbols, images, and numbers processed for analysis.
Destruction	The erasure of data, information or documents to dispose it and its content.
Disposal	Processes associated with the destruction or transfer decisions and actions in relation to data, information and documents that have reached the end of their lifecycle.
Document	An electronic or hard-copy file containing data or information.
Information	A collection of data processed, structured, and/or presented to create relevance and usefulness.
Information Asset	A collection of any type of data, irrespective of type or format that is processed for a specific function and has shared risks & ownership. The asset is the data/information held, not the format/system it is stored within.
Information Asset Administrator	The person(s) within a school or department that oversee or administer an information asset on a day-to-day basis on behalf of the Senior Information Asset Owner or Information Asset Owner.
Information Asset Owner (IAO)	The person who acts as the principal authority and has overall responsibility for an information asset and how it is managed. See Section 4.2.4 for more detail.

Term	Definition
Information Asset Register (IAR)	A centralised log of Information Assets identifying their owner, format / storage locations, and risk overview.
Metadata	Structured or semi-structured information which enables the creation, management and use of records through time and across the University.
Personal data	Any information relating to an identified or identifiable living individual.
Processing	An operation or set of operations which is performed on data or information including: <ul style="list-style-type: none"> • collection, recording, organisation, structuring or storage; • access or restriction, • adaptation or alteration; • retrieval, consultation or use; • disclosure by transmission, dissemination or otherwise making available; • Disposal by Destruction or accession to an Archive.
Record	A document maintained as evidence in pursuit of legal obligations or business activities. A record will consist of both content and metadata that sets out the context, structure & management of the record.
Record lifecycle	The existence of a record from its creation, through its use and retention, to its disposal.
Records Management	The systemic governance of data, information and documents including their creation, receipt, maintenance, use, and disposal of records.
Records system	A system or filing structure that captures, manages, and provides access to records over time.
Retention Period	The length of time a record is kept following a records Retention Trigger.
Retention Schedule	A document detailing for what length different document classifications are to be kept for based on legal requirements or business need.
Retention Trigger	An event or time from which a record's Retention Period runs.
Security classification	Defines how an information asset (and therefore all records) should be handled.
Security classification scheme	A documented systematic matrix for identifying and managing information based on its sensitivity and the level of protection required.
Senior Information Asset Owner	An executive or director level individual with responsibilities for determining how information is managed within their Faculty or Directorate. See section 4.2.5 for more detail.
Senior Information Risk Owner	The individual with delegated authority from the Vice-Chancellor to lead on, and advocate for, information security across the University. See section 4.2.1 for more detail.
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. Roles and Responsibilities

4.1 All staff. All staff have an individual and collective responsibility to practice good records management in line with this Policy. This includes:

4.1.1 identifying and applying record containing information that is classified not for public consumption (i.e. Confidential, Confidential-Sensitive or Secret) with the correct security label.

4.1.2 reporting incidents of inappropriate records management to the Information Compliance Team

4.2 Staff with additional responsibilities

4.2.1 Senior Information Risk Owner (SIRO). The SIRO must be a senior officer who reports into, or is a member of, the UEA Executive Team and/or Council. They will promote and act as an advocate for data protection compliance. They will:

4.2.1.1 review and determine the outcome of any exemption requests to existing records management regulations or procedures

4.2.1.2 review and determine the outcome of any proposals for high-risk processing activities in which the Senior Information Asset Owner or Information Asset Owner seeks to accept a risk against the advice of the Information Compliance Team.

4.2.2 Associate Director for Information Compliance is responsible for:

4.2.2.1 reviewing and updating the University's Policy and associated documents in relation to Records Management

4.2.2.2 supporting the SIRO in promoting a positive and effective culture in relation to the management of records

4.2.2.3 implementing the training of Information Asset Owners

4.2.2.4 initiating audits of Information Assets

4.2.2.5 implementing and maintaining the structure of an Information Asset Register

4.2.3 Information Compliance Team is responsible for:

4.2.3.1 advising the University's Information Asset Owners on this Policy and how to implement appropriate Records Management practices

4.2.3.2 auditing Information Assets

4.2.3.3 log and investigate reported incidents, advise on remediation and mitigation actions, and provide recommendations to prevent recurrence to information asset/data owners.

4.2.4 Information Asset Owners (IAO). IAOs are often operational managers and are responsible for:

4.2.4.1 identifying, owning and managing the information assets they oversee and ensuring these are logged accurately on the Information Asset Register.

4.2.4.2 supporting the completion of any Data Protection Impact Assessments (DPIAs) in relation to their Asset and owning any risks identified.

4.2.4.3 ensuring those accessing the Asset are adequately trained in Records Management, cyber security, and data protection

4.2.4.4 encouraging and enabling good Records Management practices in relation to their assets

4.2.4.5 escalating any major or high-risk information processing matters to the appropriate SIAO

4.2.5 Senior Information Asset Owners (SIAO). SIAOs are often executive leaders and are responsible for:

4.2.5.1 identifying IAOs within their Directorate/Faculty

4.2.5.2 encouraging and enabling good Records Management practices in their Directorate/Faculty

4.2.5.3 reviewing any proposals that include major or high-risk information processing and owning any approvals they grant.

4.2.5.4 escalating high-risk information processing matters to the SIRO

4.2.6 Information Asset Administrators (IAAs). IAAs support IAOs in the day-to-day management of an asset, they responsible for enacting the directions of the IAO or SIAO in relation to an asset.

5. Policy Statement

5.1 Information Asset Management

5.1.1 Any data, information or document held is - or forms part of - an Information Asset.

5.1.2 Information Assets are logged on the Information Asset Register and assigned to an Information Asset Owner who determines the Asset's processing and owns the associated risks.

5.1.3 Any changes to how an Asset is managed - including who can access it or who it is shared with - must be approved by the Information Asset Owner.

5.1.4 For more information about Information Asset management see the University of East Anglia's Policy for Information Risk Management.

5.2 Information Creation

5.2.1 Not all information is created equal; some has commercial, research or operational value, or evidences actions or decisions taken. Information that does not add value or evidence a decision/action does not require to be retained.

5.2.2 When creating a document, the author must assign it a sensible name that clearly identifies its content and purpose. By default, UEA does not apply standard naming conventions to documents.

5.3 Business Classification

5.3.1 The University undertakes a wide range of functions and activities that each generate information and documents. For information and documents to offer value they must have a purpose and be understood in their context.

5.3.2 The University sets out Business Classifications in the Business Classification Scheme.

5.3.3 The University does not mandate the application of a Business Classification to every document or correspondence generated.

5.3.4 The University should look to identify business classifications to records and storage areas and capture this information on the Information Asset Register.

5.4 Security Classification

5.4.1 Different types of data and information assets require different security measures. Proper classification is vital to ensuring effective data security and management.

5.4.2 Each security class listed in the summary tables below has defined data management controls which determine how information assets should be handled. These controls should be applied to all information assets held by the University.

5.4.3 At the point of creation, all University data will be classified and handled in accordance with the tables set out in Annex 1.

5.4.4 By default, all data/information assets are classed Open (accessible to the world). Data/information assets that need to be protected must be assigned an appropriate security class.

5.5 Information Storage

5.5.1 The University does not operate a single integrated storage model; data, information and documents are retained across a range of formats and platforms – both within UEA operated solutions and in those of third-party suppliers.

5.5.2 When considering the most appropriate, secure, location to store information, Information Asset Owners must balance the availability needs of the Asset against its Security Classification, confidentiality & integrity requirements.

5.5.3 To ensure Records are stored in the most appropriate location, the University has produced a guidance document for staff and students to adhere to.

5.6 Information Retention

5.6.1 The University does not need to retain every document or data point – only those that evidence a decision or business activity, or those identified by legislation as being required. Any information identified as redundant, obsolete or trivial should not be retained.

5.6.2 Information identified for retention should be retained in line with the associated business classification retention period listed on the UEA Retention Schedule.

5.6.3 The UEA Retention Schedule is publicly available via the website at:
<https://www.uea.ac.uk/about/university-information/statutory-legal-policies/records-retention-scheme-department-policies>

5.7 Information Disposal

5.7.1 Information disposal is the end of the lifecycle in which information is either destroyed or accessioned for permanent preservation in an archive.

5.7.2 It is important that record disposal is undertaken in a manner proportionate to its business classification and security classification – this information is detailed on the UEA Retention Schedule.

5.7.3 Destruction

5.7.3.1 Upon reaching the end of its Retention Period, information should be destroyed unless identified as potentially of historical interest or there is a legal need in place to retain the material further.

5.7.3.2 Destruction must be undertaken in a manner appropriate to the security classification of the information. Please see Annex 1 for more detail.

5.7.4 Archiving

5.7.4.1 Where data, information or a record has enduring public, research, historical, informational, evidential or legal value they can be permanently preserved in an Archive.

5.7.4.2 When reviewing an Information at - or approaching - the end of its Retention Period that is identified as being of potential historical interest please contact the Information Compliance Team to explore the possibility of accessioning the information to an archive.

6. Compliance and Monitoring

6.1 The University undertakes regular and routine monitoring of compliance with this Policy.

6.2 Failure to comply with this policy may result in disciplinary action, up to and including dismissal or termination of contract, in accordance with university HR and disciplinary procedures.

7. Related Documents

This Policy is supported by the below documents; these that should be read in conjunction with this Policy.

Associated Policies

- Information Risk Management Policy
- Data Protection Policy
- Artificial Intelligence Policy
- Acceptable Use Policy
- Information Access and Publication Policy
- Data Preservation Policy

Associated Documents

- UEA Retention Schedule
- UEA Business Classification Scheme
- UEA Storage Location Guidance
- UEA Naming Convention Guidance

8. Revision History

Version number	Approval date	Approval mechanism	Details of change
1.1	17/06/2010	Information Security Steering Committee	
1.2	17/04/2013	Information Security Steering Committee	
2.0	11/06/2013	Information Security Steering Committee	
2.1	10/07/2015	Information Security Steering Committee	
3.0	20/10/2015	Information Security Steering Committee	
4.0	20/09/2019	Information Compliance Steering Group	

Version number	Approval date	Approval mechanism	Details of change
5.0	31/01/2024	Information Management Board	
6.0	30/10/2025	Senior Information Risk Owner	Responsibility for approval changed to SIRO. Incorporated content formerly in the Information Classification Policy.
6.1	13/11/2025	Senior Information Risk Owner	Annex 1 added
6.2	19/02/2026	Senior Information Risk Owner	- Additional associated policies and documents added to Section 7

Annex 1 – Security Classification Scheme

Security class	OPEN	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE	SECRET
Description	Public information relating to the University. Does not contain information: that is operationally sensitive or contains personal data that cannot be made public.	Restricted to members of UEA, partner organisations and other non-University members and individuals, as authorised by information asset/data owners. Information which is operationally valuable, or contains non-sensitive or non-special category personal information, as defined by data protection legislation which cannot be made public	Restricted to members of UEA, partner organisations and other non-University members and individual, as authorised by information asset/data owners. Information which is operationally more valuable than Confidential, or contains sensitive or special category personal information, as defined by data protection legislation, or consists of a large amount of Confidential information.	Restricted to members of UEA, partner organisation and other non-University members and individuals, as authorised by information asset/data owners. Any confidential information that can have a major impact on the long-term viability or interests of the University. Information which consists of a large amount of Confidential-sensitive information.
Examples	<ul style="list-style-type: none"> • Programme and course information • Press releases • Published research • University prospectus 	<ul style="list-style-type: none"> • Personal information such as: <ul style="list-style-type: none"> ○ Job offers ○ Confirmation of academic achievements ○ Exam marks • Research data containing non-sensitive personal information, or information which is valuable, but non business-critical or significantly privacy-infringing. 	<ul style="list-style-type: none"> • Sickness records • Extenuating circumstance data • Financial records • Research data containing sensitive personal information • Trade union memberships • Criminal record data 	<ul style="list-style-type: none"> • Research data containing material classified by HM Government – or similar bodies – as secret
Risk/compliance impact ¹	Nil to Insignificant	Minor to moderate		Major to catastrophic

¹The likely impact on the University's business and reputation if appropriate security controls and data management were not applied and unauthorised person were to gain access to the information, the data were damaged or rendered inaccessible. Impact is described on the following scale: insignificant, minor, moderate, major, and catastrophic. Three elements of the security of the data are considered separately: confidentiality, integrity, and availability.

Security class		OPEN	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE	SECRET
Storage & transmission	Website	✓	✗	✗	✗
	Intranet (MyUEA)	✓	✗	✗	✗
	Email	✓	✓	✓	✗
	UEA Sharepoint (incl. Teams)	✓	✓	✓	✓
	UEA Shared Network Drives	✓	✓	✓	✓
	UEA approved Content Management System	✗	✓	✓	✓
	Third Party Solutions	✓	✓	✓	✓
	Paper	✓	✓	✗	✗
	Transmission or collaboration	Unrestricted dissemination via electronic or hard copy	<ul style="list-style-type: none"> Any distributed documents (electronic or paper) to be marked as 'Confidential' and the intended recipients clearly indicated Printed copies to be delivered by hand directly to the recipient 	<ul style="list-style-type: none"> May only be transmitted within institutional systems in encrypted format May only be transmitted outside institutional systems in encrypted format Any distributed documents (electronic or paper) to be marked as 'Confidential-Sensitive' and the intended recipients clearly indicated Printed copies to be delivered by hand directly to the recipient Appropriate 3rd party storage can be used provided encryption/appropriate security controls are in place 	<ul style="list-style-type: none"> Not normally transmitted via email, but where this is essential both the transmission and the content must be encrypted Appropriate third-party storage transmission mechanisms can be used provided encryption/appropriate security controls are in place. Information asset/data owners are advised to seek advice from ITCS in advance of using third-party transmission tools for this data class Where printed, handled according to Governance Office procedures for secret documents

Security class	OPEN	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE	SECRET
Example security measures ²	<ul style="list-style-type: none"> • Stored on departmental central file stores with restricted permissions to edit • Stored on departmental dedicated CMS with restricted permissions to edit <p>Permissions to modify limited to authorised persons, and procedures in place to ensure that information is kept up to date</p>	<ul style="list-style-type: none"> • Security measures will be appropriate to the security impact of data damage or loss • Restricted to a particular group and/or storage location, only authorised personnel allowed to have access to the information access and editing control mechanisms applied • Storage to be encrypted • Printed copies kept secure, e.g. in locked filing cabinet with only authorised individuals having access 		<ul style="list-style-type: none"> • Stored in special areas of central file stores to which only the information asset/data owner has access and only they can allow access to other authorised individuals • Document access limited at all times by encryption keys • Documents may be distributed only on paper during a meeting to review the information, and collected from all recipients before the meeting closes • Dissemination, access and handling strictly controlled by the information asset/data owner, limited to very few authorised individual and all access and handling logged in an auditable manner.
Destruction	<ul style="list-style-type: none"> • Electronic data deleted using normal file deletion processes • Printed material disposed of via non-confidential recycled waste, i.e. does not require shredding or disposal via dedicated bins for disposal of confidential material 	<ul style="list-style-type: none"> • On decommissioning of equipment used to store the data, the storage should be securely wiped to CESG Enhanced standard³, or physically destroyed. • Printed copies to be shredded in a cross-cut shredder or disposed of via dedicated bins for disposal of confidential material. • Records of disposal should be created and maintained. 		

² The listed example security measures are not exhaustive and other methods of securing data may be appropriate. Contact infosec@uea.ac.uk for advice.

³ CESG Enhanced standard – UK Communications Electronics Security Groups (CESG) Enhanced standards