Policy Type: Both internal and external

University of East Anglia Norwich

Digital Preservation Policy

Date approved:	27 February 2026
Approving body:	Senior Information Risk Owner
Date of next review:	January 2028
Review frequency:	Every 2 years
Policy/Regulation Owner:	James Bentley *Associate Director for Information Compliance and Data Protection Officer*

If you require more information about this policy/regulation, please contact the Governance Office by emailing Governance@uea.ac.uk – The Governance Office will direct your query to the relevant team or individual.

1. Overview and Purpose

1.1 The University processes information to deliver its primary purposes of teaching and research and achieve its wider strategic objectives. The University recognises the importance and value of this information both to the institution and the wider public.

1.2 This Policy is intended to establish how information intended for long-term and/or permanent preservation will be held by the University in a manner than ensures its accessibility, authenticity, and usability.

1.3 This Policy will be supported by specific guidance and training materials. This Policy should be read in conjunction with other related information management policies.

1.4 Any queries about this Policy should be directed to the University's Information Compliance Team at RecordsManagement@uea.ac.uk.

2. Scope

2.1 This Policy applies to digital materials, or materials intended to be digitised, whether created or acquired by the University, that have an ongoing legal, administrative, research, historical, or cultural value.

2.2 This policy does not replace records retention schedules, data management plans, or information security policies, but operates in alignment with them.

2.3 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.

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.
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 Owner (IAO)	The person who acts as the principal authority and has overall responsibility for an information asset and how it is managed. This term is synonymous with previously used terms including: Data Owner, and Personal Data Owner.
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: • collection, recording, organisation, structuring or storage; • adaptation or alteration; • retrieval, consultation or use; • disclosure by transmission, dissemination or otherwise making available; • alignment or combination; or • restriction, erasure or destruction.
Security Classification	Defines how an information asset should be handled, according to the Information Classification and Data Management Policy.
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.
Supervisory Authority	In the UK, the supervisory authority for requests received under the Freedom of Information and Environmental Information Regulations is the Information Commissioner's Office (ICO).

4. Roles and Responsibilities

4.1 The proper management of information is the responsibility of everyone. This section sets out the responsibilities of all users; including those at UEA with additional responsibilities.

4.2 All users

4.2.1 Any individual with access to UEA information has an individual and collective responsibility to ensure it is processed in line with the law and this Policy.

4.3 Parties with Additional Responsibilities:

4.4.1 Council. As the University's governing body, Council is responsible for ensuring the UEA has in place the necessary framework is in place to meet the legal requirements. They will delegate to the Executive Team the strategic and operational oversight for information management compliance

4.4.2 The Executive Team, as delegated by Council, has the responsibility for ensuring the University meets its legal obligations for information management compliance.

4.4.3 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:

4.4.3.1 promote and act as an advocate for information management
4.4.3.2 approve and own information management policies

4.4.4 Associate Director for Information Compliance. The person with overall responsibility for monitoring the University's compliance with information management legislation and associated internal policies. They will:

4.4.4.1 lead a central University service (the Information Compliance Team) that has responsibility for advising on records management practices

4.4.4.2 be responsible for reviewing and updating this policy and other documentation required by information management legislation.

4.4.5 Head of Open Research. The Head of Open Research provides strategic leadership for the preservation of digital research outputs and related materials, ensuring alignment with open research practice and institutional priorities. They will:

4.4.5.1 promote and embed digital preservation requirements within research workflows and guidance (including repository/deposit processes and data management planning); and

4.4.5.2 work with Information Compliance to ensure appropriate arrangements are in place for the selection, preparation and deposit of research materials requiring long-term preservation, escalating material risks or gaps to the SIRO as required.

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

4.4.6.1 identifying IAOs within their Directorate/Faculty

4.4.6.2 encouraging and enabling good Records Management and information management practices in their Directorate/Faculty

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

4.4.7.1 identifying, owning and managing the information assets they oversee.

4.4.7.2 identifying assets, or elements within them, that have an ongoing legal, administrative, research, historical, or cultural value.

4.4.7.4 ensuring any agreed assets, or elements within them, are accessioned correctly into the University's digital preservation solution

4.2.8 Information Asset Administrators. 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 Selection and Appraisal

5.1.1 Not all digital materials can or should be preserved indefinitely. Only those identified based on documented appraisal criteria should be preserved.

5.1.2 The University shall implement a documented appraisal criteria that takes into consideration: value, uniqueness, legal requirements, reuse potential, and cost of preservation.

5.2 Statutory Information Access Requests

5.2.1 The University will employ a combination of technical and organisational measures, which may include:

- Use of managed, secure storage with geographic redundancy
- Fixity checking and integrity monitoring
- Format identification, validation, and normalization where appropriate
- Documentation of provenance, metadata, and preservation actions
- Planned migration or emulation strategies to address technological obsolescence.

5.3 Metadata and Documentation

5.3.1 Preserved digital assets will be supported by sufficient descriptive, technical, administrative, and preservation metadata to enable discovery, management, and long-term usability.

5.4 Access, Rights, and Restrictions

Access to preserved digital assets will be managed in accordance with applicable legislation, licensing agreements, ethical considerations, and University policies, including data protection and intellectual property policies.

6. Compliance and Monitoring

6.1 The University undertakes regular 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
- Records Management Policy
- Information Access and Publications Policy
- Data Protection Policy

8. Revision History

Version number	Approval date	Approval mechanism	Details of change
1.0	19/02/2026	SIRO	Initial version.