Policy Type: Both internal and external

University of East Anglia Norwich

Information Risk Management Policy

Date approved:	30 October 2025
Approving body:	Senior Information Risk Owner
Date of next review:	September 2027
Review frequency:	Every 2 years
Policy/Regulation Owner:	James Bentley *Information Compliance Manager and Data Protection Officer* Steven Kennett *Chief Information Security 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 purpose of this Information Risk Policy is to establish a framework for managing information-related risks that could impact the confidentiality, integrity, or availability of university data and systems.

1.2 This ensures the university can achieve its mission of delivering 'for the public benefit, the advancement of education and research' while maintaining compliance with applicable legal and regulatory requirements.

1.3 This Policy is supported by specific guidance and training materials. This Policy should be read in conjunction with other related documents listed in Section 6.

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

3. Definitions

Term	Definition
Data	Facts, observations, statistics, characters, symbols, images, and numbers processed for analysis.
Destruction	The erasure of data, information or documents to dispose of 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.
Impact	The perceived or actual effect or consequence of an event or action.
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-today basis on behalf of the 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.
Information Asset Register (IAR)	A centralised log of Information Assets identifying their owner, format / storage locations, and risk overview.
Issue	An actual negative outcome resulting from an event or action. It is different from a Risk as it has happened or is happening.
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.

Term	Definition
Processing	An operation or set of operations 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.
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.
Records management	The systemic governance of data, information and documents including their creation, receipt, maintenance, use, and disposal of records.
Risk	A potential negative outcome resulting from an event or action. It is different from an Issue as it has not happened.
Risk Appetite	The amount of risk, by risk type, that an organisation is willing to tolerate to achieve its objectives.
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 4.2.8 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 4.2.3 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. Any individual with access to UEA data has an individual and collective responsibility to ensure data is processed in line with the law and this Policy. This includes:

4.1.1 completion of any mandatory data protection and cyber security training

4.1.2 adherence to any organisational and service data management procedures

4.1.3 supporting the Information Compliance Team, when requested, in the processing of statutory information requests

4.2 Parties with Additional Responsibilities:

4.2.1 Council. As the University's governing body, Council is responsible for ensuring the UEA has in place the necessary framework is in place to effectively manage information risks. They will:

4.2.1.1 set the University's risk appetite

4.2.1.2 delegate to the Executive Team the strategic and operational oversight for information risk management

4.2.1.3 receive and review reports on UEA's compliance position with regards to data protection and cyber security

4.2.2 The Executive Team, as delegated by Council, has the responsibility for ensuring the University meets its legal obligations for data protection and information security compliance.

4.2.3 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 promote and act as an advocate for information risk management. They will:

4.2.3.1 review and determine the outcome of any exemption requests to existing data protection policy or procedures

4.2.3.2 review and determine the outcome of any proposals for high-risk processing activities in which the Information Asset Owner seeks to accept a risk against the advice of the Data Protection Officer or Chief Information Security Officer.

4.2.4 Chief Information Officer (CIO) is responsible for:

4.2.4.1 deputising for the SIRO in their absence.

4.2.4.2 ensuring the operation of a digital estate

4.2.4.3 ensuring the adequate resourcing of an Information Security service in relation to digital assets

4.2.5 Chief Information Security Officer (CISO) is responsible for:

4.2.5.1 ensuring all electronic systems, services and equipment for processing data meet acceptable security standards

4.2.5.2 performing regular checks and scans to ensure security-related hardware and software is functioning properly

4.2.5.3 evaluating the security standards of any third-party services the University may consider using

4.2.5.4 reviewing and updating this policy in conjunction with the DPO

4.2.6 Data Protection Officer (DPO). The person with overall responsibility for monitoring the University's compliance with the Data Protection Legislation. This role may be aligned to other roles. The DPO is responsible for:

4.2.6.1 providing risk-based advice to UEA on - and monitoring – privacy, data protection and records management

4.2.6.2 being the contact point for the supervisory authority (the ICO), and for individuals whose data is processed by UEA.

4.2.6.3 attending the University's Research and Ethics Board (U-REC)

4.2.6.4 initiating data protection audits of information assets / processing activities.

4.2.7 Information Compliance Manager Is responsible for:

4.2.7.1 leading a central University service (the Information Compliance Team) that has responsibility for handling data protection related enquiries and requests, and ensuring information rights compliance

4.2.7.2 reviewing and updating this policy in conjunction with the CISO

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

4.2.8.1 identifying IAOs within their Directorate/Faculty

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

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

4.2.8.4 escalating high-risk information processing matters to the SIRO

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

4.2.9.1 identifying, owning and managing the information assets they oversee. This includes the completion of Data Protection Impact Assessments (DPIAs).

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

4.2.9.3 encouraging and enabling good Records Management practices in their area

4.2.9.4 escalating any major or high-risk information processing matters to their SIAO

4.2.10 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 Training

5.1.1 The University will provide mandatory data protection training, which will be made available to users, and other groups as appropriate as required.

5.1.2 Online training will be the default option for most staff, but face to face data protection training will be offered by the Information Compliance Team through bespoke sessions on request.

5.1.3 Individuals with responsibility under this policy must ensure that they have an understanding of the current Data Protection Legislation, information security and its impact on the University proportionate to their role.

5.1.4 Staff who have regular access to UEA computing facilities must, at minimum, complete the online data protection training available via LearnUpon which is facilitated by the Organisational Developments Services (ODS).

5.1.5 Staff who do not have regular access to UEA computing facilities will be required to complete face to face training, which will be led by the Information Compliance Team. This includes frontline staff within Cleaning and Grounds, and Catering.

5.1.6 For new staff, training must be completed prior to commencement of their duties, or at least prior to them handling any UEA Personal Data.

5.1.7 Existing staff must refresh their data protection training at least every 12 months.

5.2 Risk Management Framework

5.2.1 The University follows a risk-based approach to information risk management.

5.2.2 All information risks must be identified, assessed, and managed in accordance with the university's risk management framework.

5.2.3 The University will produce and maintain the written guidance, procedures, agreements and policies required to be able to demonstrate compliance with the information risk management practices.

5.2.4 Information risk management shall align to the University's wider risk management approach with Council defining the University's risk appetite; the Executive Team approving Risk Management procedures; and the SIRO approving information risk management policies and regulations.

5.3 Risk Assessments

5.3.1 As part of embedding a culture of privacy and security by design and default, the University must proactively undertake risk assessments of its Information Assets, any proposed changes to Assets, or any new Assets.

5.3.2 The assessment of an Asset is to be undertaken on a risk-based approach. For any Assets involving the below a full Data Protection Impact Assessment (DPIA) and/or Information Security assessment should be in place or completed before new processing commenced:

5.3.2.1 New or significantly changed systems or processes involving Personal Data or a Security Classification of Confidential, Confidential Sensitive or Secret.

5.3.2.2 Systems containing sensitive personal, financial, or research data.

5.3.2.3 Third-party vendor engagements involving university data.

5.3.2.4 Risk assessments must be documented and reviewed periodically, at least annually.

5.4 Risk Treatment

5.4.1 Any identified credible Risks and Issues must be addressed through the University treatment, transfer, tolerance, or terminate strategies.

5.4.2 All identified Risks and Issues must be documented on the appropriate DPIA and any scoring greater than 12 should be captured within the relevant Operational Risk Register.

5.5 Incident Response

5.5.1 All information security incidents must be reported immediately to the IT Service Desk, and if personal data is affected also the Information Compliance Team. All users must ensure that any suspected, potential or actual breaches are reported without delay.

5.5.2 IT and/or Information Compliance will assist with any investigations into the breach and management and containment thereof.

5.5.3 Post-incident reviews must be conducted to reassess the associated risks and improve controls.

5.5.4 If personal data is affected, the DPO and Information Compliance Team will determine whether a notification to the supervisory authority is required, and whether any affected parties should be notified.

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

- Data Protection Policy
- Records Management Policy
- Artificial Intelligence Policy

Associated Regulations

- UEA Regulations for Acceptable Computing Use

8. Revision History

Version number	Approval date	Approval mechanism	Details of change
1.0	30/10/25	SIRO	Initial Version