Policy Type: Both internal and external

University of East Anglia Norwich

Data Protection 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*

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 must process information about individuals to deliver its primary purposes of teaching and research and achieve its wider strategic objectives.

1.2 These individuals may be students, staff, and other people with whom the University has a relationship.

1.3 The University recognises the importance and value of this information and is committed to ensuring that Personal Data is appropriately processed.

1.4 This Policy is intended to establish the parameters that ensure Personal Data is processed lawfully. Specifically, the University will:

1.4.1 provide an understanding of data protection principles and requirements

1.4.2 embed data protection by design and by default

1.4.3 monitor and audit compliance with the Data Protection Legislation

1.4.4 take appropriate technical and organisational measures to secure Personal Data

1.4.5 maintain the documentation required to demonstrate compliance

b inform data subjects about how data is processed, & of their data protection rights.

1.5 This Policy is supported by specific guidance and training materials. This Policy should be read in conjunction with other related polices; and the University's privacy notices.

1.6 Any queries about this Policy should be directed to the University's Data Protection Officer at dataprotection@uea.ac.uk.

2. Scope

2.1 This Policy applies to anyone processing Personal Data on behalf of the University, and is intended to inform them about the requirements they must follow when doing so. It should be read and understood by:

2.1.1 all staff – including contractors - employed or working for UEA

2.1.2 all students who process Personal Data on behalf of the University

2.1.3 any individual who has, by virtue of their role or relationship with the University, any degree of access and/or use of Personal Data the University holds.

2.1.4 Throughout this Policy these are referred to as 'all users'.

2.2 This Policy applies to all Personal Data processed by the University, whether as a Data Controllers or as a Data Processor on behalf of a third-party. This Policy does not apply to the use of UEA devices for personal use.

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.
Data Controller	The natural or legal person who alone or jointly with others determines the purpose and means of the processing of Personal Data. UEA can be a single Data Controller, a joint-controller or a Data Processor for third-party Data Controller.
Data Processor	The natural or legal person which processes Personal Data on behalf of the controller.

Term	Definition
Data Sub-processor	A natural or legal person which processes Personal Data on behalf of a Data Processor (who in turn is doing so on behalf of a Data Controller).
Data Protection Impact Assessment (DPIA)	A risk assessment process to identify and minimise the data protection and privacy risks. DPIAs are a legal requirement where development of new or changed services, procedures or policies may present a risk to data protection or privacy.
Data Protection Legislation	All applicable data protection and privacy legislation in force from time to time in the UK including the UK General Data Protection Regulations; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended, and the guidance and codes of practice issued by the Information Commissioner or other relevant data protection or supervisory authority and applicable to a party.
Data Subject	The identified or identifiable living individual to whom Personal Data relates.
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.
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.
Lawful Basis	The conditions under which Personal Data may be processed. Processing of special category or criminal information requires a further lawful basis to be identified.
Personal Data	Any information relating to an identified or identifiable living individual.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Term	Definition
Privacy Notice	The primary means by which a Data Controller will inform the data subject how their Personal Data will be used. Usually provided in written form.
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.
Records Management	The systemic governance of data, information and documents including their creation, receipt, maintenance, use, and disposal of records.
Records of Processing Activity (ROPA)	Written records of the Personal Data processing activities undertaken by a Data Controller, as required by Article 30 of the UK GDPR.
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 data protection is the Information Commissioner's Office (ICO).

4. Roles and Responsibilities

4.1 The proper management of Personal Data is the responsibility of everyone; we all have a role to play in keeping it safe and secure. This section sets out the responsibilities of all users; including those at UEA with additional responsibilities.

4.2 All staff

4.2.1 Any individual with access to UEA Personal Data has an individual and collective responsibility to ensure data is processed in line with the law and this Policy. This includes:

4.2.1.1 completion of mandatory data protection training as directed

4.2.1.2 adherence to any organisational and service data processing procedures

4.2.1.3 supporting the Information Compliance Team, when requested, in the processing of individual rights requests.

4.3 Students

4.3.1 Student Assignments

4.3.1.1 The University is not the Data Controller for Personal Data which may be included in student coursework. This type of 'self-directed' use of Personal Data is to enable students to achieve their qualifications and the means and use of Personal Data is not determined by UEA. This type of activity would usually fall outside of the GDPR under the 'purely personal or household activity' exemption, although these students are still bound by other University policies.

4.3.1.2 However, once any coursework which contains Personal Data is submitted for marking, the UEA will be the Data Controller. In these instances, UEA's obligations are limited to what is 'practical', i.e., UEA is responsible for the security of such data but is not required to assess whether the Personal Data is accurate, minimised etc in line with the other Principles of the GDPR. The Personal Data is also not subject to Data Rights Requests under the legislation as it will be deemed to have met the exemption for examinations and scripts.

4.3.2 Students and research

4.3.2.1 Postgraduate Research students (PGR) may wish to include information about living, identifiable people in research. Additionally, Undergraduate students (UG) and Postgraduate Taught students (PGT) may wish to include information about living, identifiable people in research as part of their course/programme of study.

4.3.2.2 To establish whether UEA is the Data Controller for Personal Data collected, used and stored by these students, it is important to determine the level of instruction and guidance provided by UEA about the use of that Personal Data. UEA can only be the Data Controller for Personal Data processed by students where UEA determines the purpose and uses of the processing.

4.3.2.3 UEA is the Data Controller where a student processes Personal Data under the instruction / supervision of UEA. This policy and the Data Protection Legislation will apply to these students.

4.3.2.4 In these instances, students must abide by the instructions put in place by UEA for the handling of that data. This will ordinarily be through additional data protection checks being undertaken by UEA's Information Compliance Team when the research application progresses through the ethics approval process.

4.3.2.5 As part of their research, the student must:

4.3.2.5.1 comply with the security measures in place for the processing and storage of Personal Data

4.3.2.5.2 ensure they are up to date with GDPR training

4.3.2.5.3 refer any activities which may involve high risk or international data transfers to the Information Compliance Team before any collection or use of Personal Data commences.

4.3.3 Student Workers

4.3.3.1 Where a student is employed, or volunteering, as a member of staff at UEA (e.g., in an Ambassador or Associate Tutor role), they are acting as part of the University and thus had to comply with the requirements of UEA Staff.

4.3.4 Personal Use.

4.3.4.1 Where students use Personal Data for their own purposes (e.g., using their UEA email for their own reasons), UEA is not the Data Controller as it does not determine the purpose of such processing.

4.4 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 set out in the UK's Data Protection Legislation. They will:

4.4.1.1 delegate to the Executive Team the strategic and operational oversight for data protection compliance

4.4.1.2 receive and review reports on UEA's compliance position with regards to data protection.

4.4.2 The Executive Team, as delegated by Council, has the responsibility for ensuring the University meets its legal obligations for data protection 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 promote and act as an advocate for data protection compliance. They will:

4.4.3.1 approve and own information risk management policies

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

4.4.3.3 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.

4.4.4 Data Protection Officer (DPO). The person with overall responsibility for monitoring the University's compliance with the Data Protection Legislation. They will:

4.4.4.1 be involved, in a timely manner, in all issues relating to data protection

4.4.4.2 advise on, and monitor, data protection impact assessments (DPIA) and the DPIA process

4.4.4.3 provide risk-based advice to UEA in regard to its processing activities

4.4.4.4 act as the contact point for the supervisory authority (the ICO), and for individuals whose data is processed by UEA.

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

4.4.4.6 be responsible for reviewing and updating this policy and other documentation required by the Data Protection Legislation.

4.4.4.7 attend the University's Research and Ethics Board (U-REC)

4.4.4.8 initiate data protection audits of information assets / processing activities.

4.4.5 Chief Information Security Officer is responsible for:

4.4.5.1 ensuring all electronic systems, services and equipment for processing Personal Data meet acceptable security standards and are capable of upholding data subject rights

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

4.4.5.3 evaluating the security standards of any third-party services the University may consider using to process Personal Data

4.4.5.4 notifying the DPO without delay if a Personal Data breach is suspected or identified.

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 practices in their Directorate/Faculty

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

4.4.6.4 escalating high-risk information processing matters to the SIRO

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. This includes the completion of Data Protection Impact Assessments (DPIAs).

4.4.7.2 ensuring their staff are adequately trained in Records Management, cyber security, and data protection

4.4.7.3 ensuring adequate measures (such as a contract and/or data sharing agreement) are in place before Personal Data is shared with a third party. This includes acting as a signatory for such contracts / agreements.

4.4.7.4 encouraging and enabling good data protection practices in their area

4.4.7.5 escalating any major/high-risk information processing matters to their SIAO

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 Accountability and governance

5.1.1 The University will produce and maintain the written guidance, procedures, agreements and policies required to be able to demonstrate compliance with the Data Protection Legislation.

5.1.2 The University will pay the data protection fee, as required by the Data Protection (Charges and Information) Regulations 2018.

5.2. Data processing obligations

5.2.1 Records of Processing Activities

5.2.1.1 The University will maintain Records of Processing Activities (ROPA), as required by legislation. These Records will be subject to regular and routine review.

5.2.1.2 The University's Information Compliance Team will maintain records of activity in the following areas:

- Data breaches
- Data protection impact assessments (DPIA)
- Legitimate interest tests
- Data processing agreements (DPA)
- Information / Data sharing agreements (ISAs / DSA)
- Transfer risk assessments (TRA) and International data transfer agreements (IDTA)
- Data subject rights requests
- One-off data sharing requests
- Privacy notices
- Records retention schedules

5.2.2 Data Protection by design and by default

5.2.2.1 The University is legally required to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.

5.2.2.2 Data protection must be integrated into the University's processing activities and business practices from the design stage right through the lifecycle.

5.2.2.3 Data protection impact assessments (DPIAs) help introduce and embed data protection by design and by default. As required by the Data Protection Legislation, DPIAs will be undertaken wherever processing is considered or undertaken that is likely to result in a high risk to individuals, or if otherwise directed by the DPO.

5.2.2.4 The DPO will advise on and monitor DPIAs.

5.2.3 Data sharing

5.2.3.1 Personal Data will only be shared – including between UEA departments - where the respective purposes for processing are compatible, or where it is necessary for an applicable secondary purpose. Such re-uses should, wherever possible, identified within the privacy notice(s). Such requests must be referred to the Information Compliance Team.

5.2.3.2 The University will develop and maintain records to show where and how UEA Personal Data is shared or transferred externally to third parties.

5.2.3.3 Information Asset Owners are responsible for informing the Information Compliance Team prior to undertaking any regular or systematic data sharing activities. Where data sharing is systematic – the implementation of a data sharing agreement or data processing notice should be considered.

5.2.3.4 Unless a legal exemption applies, the nature of any data sharing must be explained to the data subject(s), ordinarily by means of a privacy notice.

5.2.3.5 Documentation establishing data processing activities with third-parties (such as contracts, data processing agreements, and information sharing agreements) should be signed by an appropriate Senior Information Asset Owner, Information Asset Owner or – in their absence – the SIRO.

5.2.4 International data transfers

5.2.4.1 UEA Personal Data must only be transferred outside the UK in accordance with the obligations set out in the Data Protection Legislation. Those involved in processing must consult the DPO where international data transfers are proposed or required.

5.2.5 Data breach management

5.2.5.1 All users must ensure that any suspected, potential or actual Personal Data breaches are reported without delay to the Information Compliance Team. They will assist with any investigations into the breach and management and containment thereof.

5.2.5.2 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.

5.2.6 Data Processing

5.2.6.1 Processing of UEA Personal Data must comply with the data protection principles that are set out in the Data Protection Legislation (Article 5 of the UK GDPR). In particular:

> **5.2.6.1.1** Privacy notices to make clear to data subjects how their data will be processed.
>
> **5.2.6.1.2** Data minimisation and accuracy to ensure that only the necessary Personal Data required for the specified purpose is collected, and that all reasonable steps are taken in relation to the accuracy of the data at all times.
>
> **5.2.6.1.3** Storage limitations to ensure data is retained by departments and data owners in accordance with their departmental Records Retention Schedules, or as required by the Research Data Management Policy.
>
> **5.2.6.1.4** Sufficient security to ensure that all appropriate technical and organisation measures are taken to protect Personal Data the University holds.

5.2.6.2 The Information Compliance Team will provide advice and guidance for all users who are required to undertake any of these activities.

5.3. Data Subject rights

5.3.1 The University will take appropriate technical and organisational measures to ensure that data subject rights, as defined by the Data Protection Legislation, are supported in the course of our processing activities.

5.3.2 All users will have sufficient understanding of the Data Protection Legislation to enable them to recognise and support data subjects in exercising their rights.

5.3.3 The University will maintain a centralised and standard process for handling all data subject rights requests. The Information Compliance Team has responsibility for handling and responding to such requests.

5.3.4 It is recognised that some rights can be supported through business-as-usual (BAU) activities, for example removing a data subject from a marketing mailing list where they have withdrawn their consent. However, where a request or a complaint relating to Personal Data falls outside the normal scope of a team's activities the DPO and Information Compliance Team must be notified without delay, to ensure the request can be handled within the statutory time period.

5.3.5 All users must also comply without delay with any data requests received from the Data Protection Officer and/or Information Compliance Team.

5.4 Marketing

5.4.1 Certain communications with staff, students and other parties may fall within the broad definition of 'marketing'.

5.4.2 Departments or data owners undertaking marketing activities must ensure that their use of Personal Data for this purpose complies with the Data Protection Legislation and the Privacy and Electronic Communications Regulations (PECR).

5.4.3 The Information Compliance Team must be consulted prior to commencing any new marketing campaign involving Personal Data.

5.5. Training

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

5.5.2 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.

5.5.3 Mandatory training requirements

5.5.3.1 Individuals with responsibility under this policy must ensure that they have an understanding of the current Data Protection Legislation and its impact on the University.

5.5.3.2 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).

5.5.3.3 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.

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

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

5.5.4 Monitoring training completion

5.5.4.1 The DPO has the overall responsibility for ensuring all users are trained in accordance with Article 39 of the UK GDPR. Responsibility for monitoring training completion is delegated to heads of departments and Schools.

5.5.4.2 Training completion records for mandatory training will be produced by ODS who will share this information with the relevant Directors, Head of Division or Head of School, to enable them to ensure training completion within their teams.

5.6 Research

5.6.1 Research projects involving Personal Data must be approved before commencement. Approval can be granted by:

5.6.1.1 a University Ethics Committee ('S-REC' or 'U-REC')

5.6.1.2 an NHS research ethics committee.

5.6.2 The Data Protection Officer is a member of the University's Research Ethics Committee (UREC) and will provide advice on data protection matters to the Committee as appropriate.

5.6.3 The Research Service within the Research and Innovation Division authorises NHS ethics applications on behalf of UEA and liaises with the Information Compliance Team on a regular basis regarding Data Protection issues.

5.6.4 Researchers should be aware of specific rules and exemptions within the Data Protection Legislation that apply to Personal Data processed for research purposes.

5.6.5 The Data Protection Officer can provide guidance and training for researchers on the specific data protection issues that apply to them.

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
- 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	30/05/12	Information Security Steering Committee	
2.0	12/06/13	Information Security Steering Committee	
3.0	20/01/15	Information Security Steering Committee	
4.0	24/05/18	Executive Team (Chair's action)	
5.0	31/01/24	Information Management Board	
6.0	01/08/24	Information Management Board (Chair's action)	Changes regarding Student research
7.0	31/10/24	Information Management Board	

8.0	19/11/24	Information Management Board (Chair's action)	Changes to signatories and Section 9 - Research
9.0	May 2025	Information Management Board	• Addition: role of Information Asset Owners & IMB • Amend: signatories for DSAs & ISAs broaden to IAOs
9.1	16/06/25	Information Management Board	Role of SIRO amended to allow for officers who 'report into ET'.
9.2	30/10/2025	SIRO	• SIAOs added • CIO changed to CISO • References to IMB removed