Data Protection Policy

University of East Anglia

Document Control Information

Title:	Data Protection Policy
Date:	1 August 2024
Version:	6.0
Authors:	Information Compliance Team
Quality Assurance:	Information Management Board (IMB)
Security Class	Open

Revision	Date	Revision Description
v.1.0	30/05/12	Approved by ISSC
v.2.0	12/06/13	Approved by ISSC
v.3.0	20/01/15	Approved by ISSC
v.4.0	24/05/18	Approved by Executive Team (Chair's action)
v.5.0	31/01/24	Approved by IMB
v.6.0	01/08/24	Approved by Chair's action (Changes regarding Student research)

Contents

Introduction

The University must gather and use certain information about individuals in order to undertake its primary purposes of teaching and research and achieve its wider strategic objectives. These individuals may be students, staff, and other people with whom the University has a relationship.

The University recognises the importance and value of this information and is committed to ensuring that personal data is processed in line with the data protection legislation and University standards and policies.

The purpose of this policy is to set out, for the benefit of UEA staff, students and other interested parties, how this personal data will be managed by the University.

The policy is supported by specific guidance and training materials that are made available to all staff. It should be read in conjunction with other related polices listed in section 10 as well as the University's privacy notices, published on our website.

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

Definition of terms

Data controller	The natural or legal person who alone or jointly with others determines the purpose and means of the processing of personal data. For the purposes of this policy, UEA is the data controller.
Data owner	The data owner is the person or department within UEA who acts as the principal authority and has overall responsibility for a collection of data and for ensuring that it is managed securely and in compliance with the University and government regulations and policies. Data may be part of an information asset and might be held in platforms used by various departments (e.g. SITS). The data owner may delegate day-to-day responsibility for management of the data to an administrator, service group or other persons.
Data processor	The natural or legal person which processes personal data on behalf of the controller.
Data protection impact assessment	A risk assessment process designed to help the University (or any organisation) identify and minimise the privacy risks presented by the development of new or changed services, procedures or policies.
Data protection legislation	All applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; 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	An information asset is a collection of any type of data, irrespective of type (e.g. numerical data, text) and format (e.g. digital or hard copy).
Information asset owner	The information asset owner is the person or department within UEA who acts as the principal authority and has overall responsibility for the information asset and for ensuring that it is managed securely and in compliance with the University and government regulations and policies. The information asset owner may delegate day-to-day responsibility for management of the data to an administrator, service group or other persons.

Lawful basis	The condition under which personal data may be processed. The lawful bases are defined in Article 6 of the GDPR. Processing of special category requires a further lawful basis to be identified.
Personal data	Any information relating to an identified or identifiable living individual.
Personal data asset	A personal data asset is a type of information asset; it is a collection of personal data, irrespective of type (e.g. numerical data, text) and format (e.g. digital or hard copy).
Personal data asset owner	The personal data asset owner is the person or department within UEA who acts as the principal authority and has overall responsibility for the personal data asset and for ensuring that it is managed securely and in compliance with the University and government regulations and policies. The personal data asset owner may delegate day-to-day responsibility for management of the data to an administrator, service group or other persons.
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.
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	In relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as: • 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 of processing activity	Written records of the personal data processing activities undertaken by a data controller, as required by Article 30 of the GDPR.
Security class	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).

1. Policy principles

This Policy is based on the principle that the University will ensure processing of personal data for which UEA is the data controller (including joint controller) or a processor meets the standards and requirements of the data protection legislation.

Specifically, the University will:

- Equip staff with an understanding of data protection principles and requirements
- Embed data protection by design and by default as a collective responsibility
- Monitor and audit its compliance with the data protection legislation
- Take appropriate technical and organisational measures to secure personal data
- Maintain the documentation required to demonstrate our compliance

- Provide clear information to enable people whose data is processed by the University to understand
    - how their data will be used, and
    - their data protection rights
- Adopt relevant codes of practice and guidance produced by the supervisory authority.

2. Scope

This policy applies to:

- All staff employed by UEA
- All students who have access to, or who are processing personal data for which the University is the data controller or processor
- 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
- All University activities that involve the processing of personal data as defined by the data protection legislation

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

3. Responsibility

3.1 All staff

Data protection compliance is the responsibility of the data controller. This means all staff and other parties who may access or use UEA personal data have an individual and collective responsibility to ensure they can demonstrate the data is processed in line with the law and this policy.

Where staff or other individuals are also data owners, they must be aware of their specific responsibilities, as described in this and other policies, listed in section 10.

The following members of staff have specific areas of responsibility:

3.1.1 The Executive Team

The University's Executive Team consists of the Vice-Chancellor, the Deputy Vice-Chancellor, six Pro-Vice-Chancellors, the Chief Resource Officer, the Director of Finance, and the Director of People and Culture. The Executive Team has the responsibility for ensuring the University meets its legal obligations on behalf of Council.

3.1.2 Data Protection Officer (DPO)

At UEA, the person with overall responsibility for monitoring the University's compliance with the data protection legislation, including awareness raising, training and audits, is the Data Protection Officer. According to the law, the DPO is independent, reports directly to the highest management level of the University and will:

- Be involved, in a timely manner, in all issues relating to data protection at UEA
- Advise on, and monitor, the data protection impact assessment (DPIA) process
- Provide risk-based advice to the University in regard to its processing activities
- Act as a contact point for the supervisory authority (the ICO), and for individuals whose data is processed by UEA

The DPO will also:

- 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
- Be responsible for reviewing and updating this policy and other documentation required by the data protection legislation.

3.1.3 Director of ITCS

Is responsible for:

- Ensuring all systems, services and equipment used for processing personal data meet acceptable security standards and are capable of upholding data subject rights
- Performing regular checks and scans to ensure security-related hardware and software is functioning properly
- Evaluating the security standards of any third-party services the University may consider using to process personal data
- Notifying the DPO without delay if a personal data breach is suspected or identified.

3.1.3 Heads of Department/School

Are responsible for:

- Ensuring their staff complete the data protection training, as detailed in section 7
- Identifying and supporting a member of their team to act as the nominated data protection contact for their area (see 3.1.4)
- Encouraging and enabling good data protection practices in their area.

3.1.4 Data Protection Contacts

The University has a network of data protection contacts, who work with the Data Protection Officer and Information Compliance Team to ensure the University complies with the data protection legislation. They will:

- Where required, facilitate data subject rights requests on behalf of and as directed by the Information Compliance Team
- Forward any complaints or concerns about personal data handling to the DPO and Information Compliance Team

3.2 Students

Unless they are also acting as a member of staff (e.g., in an Ambassador or Associate Tutor role), students will not normally be expected, or able, to access or process UEA personal data.

The University is not the Data Controller for incidental personal data which may be included in student coursework (except for that included in the 'Students and Research' section, below). 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. Likewise, 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.

However, once any coursework which contains incidental 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.

Students and research

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.

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.

UEA is the Data Controller where: A student processes personal data under the instruction/supervision of UEA, e.g., (a) as part of their UG dissertation project or coursework, or (b) as part of their PGT dissertation project or coursework, or (c) as part of their PhD studies. 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.

In accordance with the 'Guidance for UEA students processing personal data as part of their research', the student must comply with the security measures in place for the processing and storage of personal data, ensure they are up to date with GDPR training, and 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. This policy and the data protection legislation will apply to these students.

4. Accountability and governance

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. Such records will be made available to the supervisory authority on demand and published where possible to enhance transparency.

The Data Protection Officer and Information Compliance Team will be responsible for creating and monitoring statutory documentation and will assist departments in drafting and maintaining specific guidance and procedures.

4.1 Notification fee

The University will pay the data protection fee, as required by the Data Protection (Charges and Information) Regulations 2018. The DPO will be responsible for administration of fee payment.

4.2 Records of Processing Activities

The University will maintain Records of Processing Activities (ROPA), as required by the data protection legislation. These Records will be subject to at least annual review. Reviews will be led by the Information Compliance team, with assistance from data protection contacts where necessary.

The University will adopt current supervisory authority guidance and templates when reviewing its ROPA and will seek to use technology where possible to maintain and improve accuracy of the Records.

In addition to the ROPA, 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)
- Data sharing agreements (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 (RRS)

4.3 Data Classification

To assist with identification and protection, information assets containing personal data, i.e. personal data assets are to be classified according to the Information Classification and Data Management Policy.

4.4 Audits

The DPO will, where required and according to any defined and agreed schedule, undertake audits of data processing practices across the University. Aspects of this task may be delegated to senior staff within the Information Compliance Team.

4.5 Data sharing and transfers

The University will develop and maintain records to show where and how UEA personal data is shared or transferred externally to third parties, in particular where overseas transfer of data is required.

Data owners are responsible for informing the Information Compliance Team prior to undertaking any regular or systematic data sharing activities.

Unless a legal exemption applies, the nature of any data sharing must have been explained to the data subject(s), ordinarily by means of a privacy notice (see section 5).

Appropriate technical and security measures, such as those described in the Information Classification and Data Management Policy, must be applied to all personal data shared with external parties.

International data transfers

UEA personal data must only be transferred outside the UK in accordance with the obligations set out in the data protection legislation, in particular Chapter V of the UK GDPR. The data owner must consult the DPO where international data transfers are proposed or required.

Data sharing documentation

Data owners are responsible for ensuring adequate written contracts are in place before UEA personal data is shared with a data processor acting on behalf of the University.

Where data is shared on a joint-controller basis, the data owner is responsible for ensuring that the respective compliance obligations are agreed and documented in a transparent manner.

The Information Compliance Team is responsible for monitoring and assessing data sharing activities and agreements. The team will provide guidance on compliance with the data protection legislation, noting that legal advice may be required in some circumstances. The team may refer data owners to the Information Security Team within ITCS where appropriate, to ensure the technical security of the proposed sharing/transfer.

Authorised signatories

Only certain members of University staff will be authorised signatories for data sharing (controller-controller) and data processor agreements:

- The Senior Information Risk Officer, and
- The Contracts Manager for the Research and Innovation Division

Ad hoc disclosure of Personal Data to third parties

Ad hoc or one-off disclosure of UEA personal data to external parties will only be made where:

- Consent from the data subject is obtained and recorded, or
- Disclosure is otherwise necessary, and permitted by the data protection legislation or required by another law

Student attendance and qualification verification

Third parties may contact the University to confirm whether or not a named individual has attended the University, and whether or not they obtained a particular qualification. These queries should be directed to Student Records for a response in the first instance.

There may be circumstances under which the University will disclose information without first obtaining consent. These and any other queries must be referred to the Information Compliance Team.

Internal data sharing

Personal data held by one UEA department will only be shared with another UEA department where the respective purposes for processing are compatible (and known to the data subject), or where it is necessary for an applicable secondary purpose as provisioned by the privacy notices such as archiving purposes in the public interest, scientific research purposes, or statistical purposes, or other relevant legislation, e.g. health and safety. Such requests must be referred to the Information Compliance Team.

4.6 Data Protection by design and by default

The University is legally required, under Article 25 of the GDPR, to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This means that data protection must be integrated into the University's processing activities and business practices from the design stage right through the lifecycle.

Data protection impact assessments (DPIAs) are a key way to 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, for example, where special category data is involved.

The DPO will advise on and monitor DPIAs, as noted in section 3.1.2.

4.7 Data breach management

All University staff 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.

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. Data processing obligations

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:

- Privacy notices to make clear to data subjects how their data will be processed.
- 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.
- 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.
- Security to ensure that all appropriate technical and organisation measures are taken to protect Personal Data the University holds.

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

6. Data Subject rights

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.

All users will have sufficient understanding of the data protection legislation to enable them to recognise and support data subjects in exercising their rights.

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

7. Training

The University will provide online and face to face data protection training, which will be made available to staff and research postgraduates, and other groups as appropriate and on request.

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.

7.1 Mandatory training requirements

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.

All 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) in the People and Culture department.

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.

For new staff, training must be completed prior to commencement of their duties, or at least prior to them handling any UEA personal data. Existing staff must refresh their data protection training each year.

All users who are not permanent members of staff and who confirm they have completed, within the past year, data protection training provided by another reputable body (for example the NHS), do not need to complete UEA training. In these circumstances, the University department responsible for the individuals must ensure that they are provided with UEA guidance, procedures and policies relating to data protection. The department is also responsible for confirming the individual's external training has been refreshed each year.

7.2 Monitoring training completion

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.

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

8. Research

Research projects involving personal data must first be approved by a University Ethics Committee. 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.

Researchers should be aware of specific rules and exemptions within the data protection legislation that apply to personal data processed for research purposes. The Data Protection Officer can provide guidance and training for researchers on the specific data protection issues that apply to them. For information on students undertaking research, please see Section 3.2 of this Policy.

9. Marketing

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

The Information Compliance Team must be consulted prior to commencing any new marketing campaign involving personal data.

10. Other relevant policies

- The Conditions of Computer Use
- The General Information Security Policy
- The Information Classification and Data Management Policy
- The Records Management Policy
- The Freedom of Information Policy

11. Review process

This Policy will be reviewed by the University's Data Protection Officer every two years, or sooner as necessary. Policy approval will be sought from the Information Management Board (IMB).