Data Protection Policy

University of East Anglia

Report Control Information

Title:	Data Protection Policy
Date:	24 May 2018
Version:	4
Authors:	Information Compliance (EP)
Quality Assurance:	Executive Team (this version only)
Security Class	Open

Revision	Date	Revision Description
v.1	30/05/12	Approved by ISSC
v.2	12/06/13	Approved by ISSC
v.3	20/01/15	Approved by ISSC
v.4	24/05/18	Approved by Executive Team (Chair's action)

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 primary 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 Protection Legislation	The General Data Protection Regulation (EU) 2016/679 (as incorporated in the Data Protection Act 2018), and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any guidance or codes of practice issued by the Information Commissioner or any other designated Supervisory Authority in the UK from time to time (all as amended, updated or re-enacted from time to time).
Personal Data	Any information relating to an identified or identifiable living individual.
Data Subject	The identified or identifiable living individual to whom personal data relates.
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.
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.
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 Processor	The natural or legal person which processes personal data on behalf of the controller.
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.
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.
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.
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.
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.
Supervisory Authority	In the UK, the Supervisory Authority for data protection is the Information Commissioner's Office (ICO).
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).
Data Owner	The Data Owner is the person or department within UEA who acts as the principle authority and has overall responsibility for the information asset and for ensuring that it is managed securely and in compliance with University and government regulations and policies. The Data Owner may delegate day-to-day responsibility for management of the data to a Data Administrator, service group or other persons.
Security class	Defines how an information asset should be handled, according to the Information Classification and Data Management Policy.

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 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 and European Data Protection Board (Article 29 Working Party)

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 (UEA Personal Data)
- Any individual who has, by virtue of their role or relationship with the University, any degree of access and/or use of UEA Personal Data
- All University activities that involve the processing of Personal Data as defined by the Data Protection Legislation

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 Senior Management Team consists of the Vice Chancellor, five Pro-Vice Chancellors, the Deputy Vice Chancellor, the Chief Operating Officer and the Chief Resource Officer, and has 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, who is also the Head of Information Compliance. 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 3.3)
- 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 their areas comply with the Data Protection Legislation. They will:

- Make themselves known to their colleagues as the departmental Contact, and, where appropriate, act as an initial point of reference for colleagues with data protection queries or concerns
- Ensure the Data Protection Officer is involved, in a timely manner, in all issues relating to data protection within their area
- Where required, facilitate Subject Access 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

- Disseminate, as appropriate, any data protection guidance produced or shared by 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.

Students and research

If students undertake research involving living identifiable individuals for their own personal academic purposes then the University is not the Data Controller for the data they collect and use, and this policy does not apply. Such students are responsible for ensuring their research complies with the Data Protection Legislation, where it applies to them, and will still require ethical approval for their work.

In contrast, students working on research involving living identifiable individuals that is led by a University research group will likely be handling personal data for University purposes, provided they work under instruction from the University. This policy and the Data Protection Legislation will apply to these students.

In both scenarios, once work has been submitted for assessment the University will be responsible for processing the Personal Data within the work, in accordance with the Data Protection Legislation and this policy.

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 logs of activity in the following areas:

- Data breaches
- Data Protection Impact Assessments
- Data controller-processor contracts

- Controller-controller arrangements
- Complaints regarding processing of personal data
- Records of consent
- Privacy notices

4.3 Data Classification

To assist with identification and protection, Information Assets containing Personal Data 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), by means of a Privacy Notice (see section 5.1).

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 not be transferred outside the EEA unless the transfer complies with the obligations set out in the Data Protection Legislation, in particular Chapter V of the GDPR. The DPO must be consulted where regular or systematic 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 will 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 Chief Officers, 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 allowed 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.

In general, the University will seek consent from the individual for confirmation of attendance and verification of qualifications to third parties wherever possible before a response is provided.

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

- Potential fraudulent claims: Where an individual has made a false claim regarding attendance, employment or qualifications gained at UEA, and the University has no record of that individual having attended the institution, the enquirer will be informed.
- Other types of request: Where the University can confirm employment, student attendance or qualifications, and has not obtained explicit consent, the University will only disclose that information to verified and legitimate enquirers under certain limited circumstances where there is significant advantage to the data subject in so doing.

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 the secondary purpose is for: archiving purposes in the public interest; scientific research purposes; or statistical purposes.

4.6 Privacy by design and by default

The University will, wherever possible, seek to embed the principles of Privacy by Design, following guidance produced by the Supervisory Authority, and adopting best practice identified across the sector.

Data Protection Impact Assessments (DPIAs) are a key way to introduce and embed Privacy by Design. 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 be responsible for DPIAs, as noted in section 3.1.2.

4.7 Data breach management

All people with responsibility under this policy must ensure that any suspected, potential or actual Personal Data Breaches are reported without delay to the Information Compliance team. They will assist the DPO and any Incident Team with their investigations into the breach.

The DPO and Information Compliance team will:

- Publish guidance on what constitutes a Personal Data Breach
- Publish contact details and documentation to enable rapid breach reporting, including out of hours
- Maintain breach procedures and a standard means of assessing and logging breaches (see 4.2)
- Notify key personnel, who will form the breach Incident Team (where the severity of the breach requires this)
- Where applicable, work with ITCS, in particular the Information Security team, to assess and limit impact of breach, and reduce risk of recurrence
- Report breaches, as required, to the Supervisory Authority, and affected parties
- Provide advice and guidance on reducing the risk of similar breaches occurring

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 GDPR). In particular:

5.1 Privacy notices

The University will make clear to Data Subjects how their data will be processed. The primary means of providing this information will be via a written Privacy Notice. The University publishes 'primary' notices designed cover the majority of data processing activities and data subject groups. 'Secondary' notices will only be provided where the purposes and/or data subjects are sufficiently distinct that a separate notice is required.

Primary notices will be reviewed at least annually, and are the responsibility of the DPO. Secondary notices are the responsibility of the Data Owner, but must also be reviewed, approved and logged by the Information Compliance team prior to use. The exceptions to this requirement are the information sheets provided to research participants; these are reviewed and logged by the University's ethics committees.

The Information Compliance team will provide advice and guidance for staff who are required to draft a privacy notice.

5.2 Data minimisation and accuracy

Data Owners must ensure that they collect and use only the least amount of data required for the specified purpose, and that they take all reasonable steps to confirm the accuracy of the data.

5.3 Storage limitations

Personal data will be retained by departments and Data Owners in accordance with their departmental Records Retention Schedules, or as required by the Research Data Management Policy. Any documented retention schedule or policy must be kept up to date and accessible to the Data Subjects.

Data must be stored securely when it is not being actively processed and is held in on or off-site storage. Data Owners must ensure that appropriate access controls are in place.

As soon as data is no longer required to be held in a format that identifies individuals, it will be pseudonymised, anonymised or securely deleted or destroyed. According to the law, research data may be retained for longer periods, provided it is appropriately protected.

5.4 Security

All individuals with responsibility under this policy must take appropriate technical and organisation measures to protect UEA Personal Data. Although ITCS has responsibility for many of the technical

security measures applied to UEA systems (see section 3.1.3) holding digital data, individuals also have a responsibility to protect Personal Data held in both digital and hard copy. For example:

- Undertake Information Security training (available via Blackboard) where required, to improve awareness of risks
- Have an understanding of UEA security policies and the technical security measures applied to the data under their control, and ask questions (of ITCS or external parties) where this is not clear
- Apply appropriate access controls to Personal Data
- Undertake regular reviews of physical security and office layout, including enforcement of a clear desk policy
- Where Personal Data is to be processed using an IT solution, ensure that system is supported and approved by ITCS
- Apply encryption or password protection to information assets, as advised by ITCS and UEA policy

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 people with responsibility under this policy will have sufficient understanding of the Data Protection Legislation to enable them to recognise and uphold Data Subjects in exercising their rights.

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 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.

The Information Compliance team will follow documented procedures for handling and recording complaints and requests, and respond within the time period allowed by the Data Protection Legislation.

Subject Access Requests

The University will maintain a centralised and standard process for handling Subject Access Requests. The Information Compliance team has responsibility for handling and responding to such requests. All requests for personal data that fall outside BAU must be directed to the DPO and Information Compliance team without delay, to ensure the request can be handled within the statutory time period.

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 via the Centre for Staff and Educational Development (CSED), or 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 Blackboard.

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.

Individuals with responsibility under this policy 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

Department heads and heads of Schools are responsible for ensuring their staff complete the training.

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

8. Research

Research projects involving human subjects 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.

As noted in 5.3, Personal Data held for research purposes may be held for longer than other types of data. Nonetheless, researchers should ensure that personal data is stored for no longer than is required, and is pseudonymised or anonymised where possible.

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 will provide guidance and training for researchers on the specific data protection issues that apply to them.

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, in particular that the Data Subject has been notified via a Privacy Notice, that the correct Lawful Basis has been identified, including seeking consent where necessary, and that procedures are in place to support Data Subjects' rights.

Data Subjects have the right to object to direct marketing, and departments must cease this activity if an individual objects, or withdraws their consent.

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

The University's Data Protection Officer will undertake a biennial review of this policy, or revise as required to reflect significant external and internal changes. Policy approval will be sought from the Information Strategy and Services Committee (ISSC).