University of Essex

Data Protection Policy

Authors:	Information Assurance Team
Publication date:	December 2022
Amended:	September 2022
Review date:	August 2024

Table of Contents

Data Protection Policy

1. Introduction

This policy sets out how the University of Essex will process the personal data of its data subjects including staff, students, alumni, research participants, suppliers, visitors and other third parties.

The aim of this policy is to ensure that everyone handling personal data is fully aware of their responsibilities and the University's legal obligations under the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR), together the data protection legislation. Its aim is also to ensure that everyone handling personal data does so in accordance with data protection principles and procedures, and our Privacy Policies.

Data Protection has a crucial role to play in ensuring that the University maintains the trust and confidence of all members of its community, including students, staff, alumni, visitors, partners and other third parties.

The University of Essex is registered as a Data Controller with the UK's Information Commissioner's Office (ICO), registration number: Z699129

2. Scope and Definitions

This policy applies to all staff including contractors who store, share, access, handle or otherwise process personal data.

The policy applies to students where they are processing personal data on behalf of the University but not where they are processing personal data for non-University or private purposes.

Compliance with this policy and the related policies and procedures listed in this policy, and also included in the Annex, is mandatory. Any breach of this policy and any related policies and procedures may result in disciplinary action.

A glossary of the terms used throughout the Policy can be found in Appendix 1.

3. Responsibilities

3.1 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for: advising the University of its data protection obligations under the law; monitoring University compliance with the law; and monitoring University compliance with this policy and any related policies. They shall:

- inform and advise all members of staff on their data protection obligations;
- monitor compliance with data protection requirements;
- contribute to the development and maintenance of all data protection policies, procedures and processes in relation to the protection of personal data;
- advise and inform the University on any data protection impact assessment (DPIA), including monitoring performance of DPIAs;
- implement appropriate data protection training;
- conduct audits of processes relating to personal data;
- be the point of contact for data subjects about the processing of their personal data and respond to all data subject access requests;
- ensure that records of the processing are kept;
- advise on the issuing of privacy notices to data subjects at the point of collection of their personal data; and
- be the first point of contact for any enquiries from the Information Commissioner's Office (and any EU supervisory authorities, where relevant).

3.2 Registrar and Secretary

The Registrar and Secretary has overall responsibility for the strategic and operational management of privacy and data protection compliance. They shall:

- champion a data protection culture in the University;
- ensure that adequate resources are devoted to meet the University's data protection obligations;
- commission reports from the Data Protection Officer and take action to remedy deficiencies identified by the report in a timely manner; and
- ensure the Data Protection Officer operates independently and is not dismissed or penalised for performing their task (in relation only to their role as Data Protection Officer as defined in law).

3.3 All staff

- All staff, across all departments of the University must read, understand and comply with this Policy when processing personal data when performing their tasks. They must observe and comply with all controls, practices, protocols and training to ensure such compliance. All staff must:
- ensure any personal data which they hold is kept securely;

- ensure personal information is not disclosed either orally or in writing, accidentally or otherwise unlawfully to any unauthorised party;
- ensure they share data in compliance with the data protection principles e.g. taking into account the requirement for data minimisation, fairness etc. (see 4. below for a full list of principles)
- only access personal data that is applicable and required for them to undertake their role;
- report a data breach immediately when any data breach occurs;
- undertake all required data protection/cyber security training;
- maintain data protection awareness at all times, reporting any data protection risks or concerns to their Line Manager or the Data Protection Officer;
- ensure that records are accurate, kept up to date, kept securely and disposed of safely in accordance with the timescales set out in this and other relevant record keeping procedures;
- ensure they have an appropriate contract in place (approved by the Data Protection Officer) with any third-party organisation that will have access to personal data;
- where staff are required to send personal data to another country or international organisations, they must seek advice from the Data Protection Officer; and
- follow all guidance relating to information sharing.

4. Data Protection Principles

The University and its staff must comply with the data protection principles by ensuring that data is:

- processed lawfully, fairly and in a transparent manner;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed;
- accurate and, where necessary, kept up to date;
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Additionally, the University and its staff must ensure that:

- personal data is not transferred or exposed outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place; and
- data subjects are allowed to exercise their rights in relation to their personal data.

The University and its staff are responsible for, and must be able to demonstrate compliance with, all the above principles.

5. Processing data lawfully

In order to process personal information, the University must meet one of the legal bases contained within Article 6(1) of the UK GDPR. In order to process special category personal information, the University must also meet one of the legal bases contained within Article 9(2).

The legal basis for processing must be determined before the processing commences. The legal basis must also be recorded, for example through a Data Protection Impact Assessment or within the University's suite of Privacy Notices.

5.1 Lawful basis for processing

For the processing of personal data to be legal under the data protection legislation, the University must determine under which legal basis the data is being processed.

There are six legal bases listed in Article 6(1) of the UK GDPR:

a) Consent: the data subject has given clear consent for you to process their personal data for a specific purpose

b) Contract: the processing is necessary for a contract you have with the data subject, or because they have asked you to take specific steps before entering into a contract

c) Legal Obligation: the processing is necessary for you to comply with the law

d) Vital Interests: the processing is necessary to protect someone's life

e) Public Task: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University

f) Legitimate Interests: processing is necessary for the purposes of the legitimate interests pursued by the University or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.2 Lawful basis for processing special category data

The University is prohibited from processing special category data (as defined by the GDPR) unless, in addition, to one of the grounds above a second ground applies. These grounds set out in the GDPR (as supplemented by the Data Protection Act 2018) are:

a) Explicit Consent: the data subject has given explicit consent to the processing of special category data for one or more specified purposes

b) Obligations and Rights: processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the University or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by UK law

c) Vital Interests of the data subject or another person: processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

d) Legitimate Activities: processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

e) Public Domain: processing relates to personal data which are manifestly made public by the data subject

f) Legal Claims: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g) Substantial Public Interest: processing is necessary for reasons of substantial public interest, with a basis in UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

h) Health and Social Care: processing is necessary for reasons of substantial public interest, with a basis in UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

i) Public Health: processing is necessary for reasons of substantial public interest, with a basis in UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

j) Archiving / Research: processing is necessary for reasons of substantial public interest, with a basis in UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5.3 Criminal convictions data

Where the University processes personal data relating to criminal convictions and offences or related security measures, it must do so in accordance with the law and provide appropriate safeguards for the rights and freedoms of data subjects.

Schedule 1 of the Data Protection Act 2018 provides further information as to when special category and criminal convictions and offence data can be lawfully processed.

5.4 Fair processing of personal data

Processing of personal data must always be fair as well as lawful. Even if the University can show that it has a lawful basis for the processing (as explained above) it does not automatically mean the processing is fair.

In general, fairness means that the University will only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. The University's privacy hub, containing our Privacy Notices, describes how we will process personal data.

All staff should think not just about how they can use personal data, but also about whether they should. When sharing personal data, especially special category (sensitive) data, staff should ensure the use of the data is appropriate and should consult with the Data Protection Officer (DPO) for additional advice and guidance (where necessary).

6. Privacy Notices / Fair Processing Notices

The concept of transparency runs throughout the GDPR and requires the University to ensure that any information provided by the University to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language.

The University has developed a suite of Privacy Notices, which cover the University's processing activities. These are available from the University's Privacy Hub.

7. Purpose Limitation

The University must only collect and process personal data for specified, explicit and legitimate purposes that are provided to data subjects through easily accessible privacy information, available in advance or at the time that the personal data is collected. The purposes must correspond with the appropriate lawful basis on which the University is seeking to rely.

The University and its staff must ensure that they do not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose without undertaking steps in line with their obligations under data protection legislation. Where the University intends to do so, it must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

There are limited exceptional circumstances under which data may be repurposed. Please obtain advice from the DPO.

8. Data minimisation

The personal data that the University collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

This means that the University must:

- only collect personal data actually needed for the specified purposes;
- ensure it has sufficient personal data to fulfil properly those purposes; and
- periodically review the data it holds and delete anything in line with retention schedules.

Staff should always ensure that they do not have more personal data than needed to achieve the purpose for which the data is being processed, and not share excessive personal data or include irrelevant/excessive details when the data is being shared, and not share the data more widely than is necessary.

9. Accuracy

The personal data that the University and its staff collects, and processes must be accurate and, where necessary, kept up–to-date, and must be corrected or deleted without delay if the University discovers, or is notified, that the data is inaccurate.

Staff must update all relevant records if they become aware that any personal data is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

10. Storage limitation

The personal data that the University collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

Storing personal data for longer than necessary may increase the likelihood and severity of a data breach and may also lead to increased costs associated with such storage.

The University must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

Staff must observe and comply with the University's Information and Records Management policies and procedures.

11. Security, integrity and confidentiality

The personal data that the University and its staff collect and process must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

Staff are responsible for ensuring the security of the personal data they process in the performance of their duties and tasks. Staff must ensure that they follow all procedures that the University has put in place to maintain the security of personal data from collection to destruction.

Staff must not attempt to circumvent any administrative, physical or technical measures the University has implemented as doing so may result in disciplinary action and, in certain circumstances, may constitute a criminal offence.

11.1 Reporting personal data breaches

In certain circumstances, the GDPR will require the University to notify the Information Commissioner's Office (ICO), and potentially data subjects, of any personal data breach. The University will notify the ICO and/or data subjects where the University is legally required to do so should a notifiable breach occur.

If staff know or suspect that a personal data breach has occurred, they must immediately report it to the Data Protection Officer and take all appropriate steps to preserve evidence relating to the breach. If necessary, staff should obtain data protection advice from the DPO. The Information Assurance Team maintains the University's data breach log including actual and suspected breaches and near misses.

Staff must observe and comply with the University's Data Breach Response Policy.

12. Sharing personal data

Staff are not permitted to share personal data with third parties unless there is a lawful basis to do so, and any processing is in accordance with the relevant data protection principles, such as data minimisation. Usually, the sharing will have been communicated to the data subject in a privacy notice or fair processing notice beforehand. Consideration should be given to the drafting of a data sharing agreement. In 'joint controller' sharing situations there must be an agreement.

Where a third party is processing the personal data on its behalf, the University must undertake due diligence on them and enter into an agreement with the processor that complies with the GDPR's requirements for such agreements ("data processing agreements"). The Data Protection Officer can offer advice in relation to these agreements.

13. Transfers outside of the European Economic Area (EEA)

The GDPR prohibits the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects as countries within the EEA do.

In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

The University and its staff may only transfer personal data outside the EEA in a number of certain situations.

Staff must ensure that staff do not transfer any personal data outside the EEA unless the University has agreed to this in advance.

Staff should seek advice from the Data Protection Officer before transferring any data outside the EEA.

14. Data Subject Rights Requests

The GDPR provides data subjects with a number of rights in relation to their personal data. The University will only have one month to respond to requests for individuals' personal data in most circumstances, in line with the applicable laws.

All Data Subject Access Requests must be fielded via the DPO and the Information Assurance team. All staff must observe and comply with the University's Data Subject Access Request Procedure.

15. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing that is likely to result in high risk to the individuals and their personal data, and where new technologies are involved. In practice, the University requires a DPIA for any projects or processes involving the use of personal data, including new systems, solutions and some research studies.

The University's Data Protection Impact Assessment Policy provides full details and a template for conducting a DPIA.

Appendix 1 – Definitions

Term	Definition
GDPR	The GDPR is the General Data Protection Regulation, which came into force on 25 May 2018. In the UK, it is referred to as UK GDPR. It sits alongside the Data Protection Act 2018. The aim of GDPR was to harmonise and strengthen data protection rules across EEA member states. It applies to data processing carried out by individuals and organisations operating within the EEA, but also applies to organisations outside the EEA that offer goods and services to EEA citizens.
Personal data	Personal data is information, in digital and analogue forms, that relates to a living identifiable person, who can be identified from that data, or from that data when combined with any other information we hold. Personal data includes information about employees, students, contractors and visitors such as: ■ names, addresses, phone numbers and emails ■ bank details ■ expressions of opinion about a person ■ mailing and events lists ■ car parking administration details ■ posts on social networking sites ■ photographs
Special category data	Special category data is defined as personal data revealing: ■ racial or ethnic origin ■ political opinions ■ religious or philosophical beliefs ■ trade union membership

Term	Definition
	■ genetic data ■ biometric data (where used for identification purposes) ■ data concerning health ■ data concerning a person's sex life; and ■ data concerning a person's sexual orientation.
Data Controller	Any person, or organisation, which makes decisions about how and why data is processed. A data controller must be a person recognised in law and they are responsible for compliance. The University of Essex is a Data Controller.
Data Processor	Any person, or organisation, which acquires, records and processes personal data or who processes data on behalf of the Data Controller. An organisation can be both a Data Controller and Data Processor even where they may appoint third parties to carry out elements of data processing on their behalf, such as Cloud Computing services. The University of Essex is both Controller and Processor. Our third parties who handle data for us are Data Processors.
Data Subject	A living person who is the subject of personal data. There are strengthened rights for individuals over their personal data that the University holds or collects. Individuals can request that we make changes in how their data is handled and we must respond promptly should a request be made.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Organisations are required to report a data breach that creates a risk to the rights and freedom of the individuals concerned to the Information Commissioner's Office (ICO) within 72 hours of the breach occurring or when made aware of the breach. If the individuals are at high risk of potential harm, then they must also be notified. Example: A computer account is hacked, and data listing contact details is accessed; or a member of staff takes unencrypted data out of the office against acceptable use policy and loses it. All data

Term	Definition
	breaches much to reported to the DPO. *See the Data Breach policy.*
Data Protection Officer (DPO)	This role in an organisation is held by the person with responsibility for ensuring that personal data is protected and that the organisation is compliant with the legislation. There should be a degree of independence in the role allowing the DPO to report directly to the senior management level of the organisation as a part of the organisation's governance. Our Data Protection Officer can be contacted at dataprotectionofficer@essex.ac.uk.
Data Subject Access Request (DSAR)	The request by an individual to have access to, and information about, the personal data that we hold about them. Application for a Data Subject Access Request is made by the individual or by an individual with authority to act on behalf of another (for example through Power of Attorney or with written authority). DSARs are free of charge. *See the Data Rights Policy.*

Policy Information

Title	**Data Protection Policy**
Policy Classification	Policy
Security Classification	Open
Policy Manager Role	Data Protection Officer
Responsible UoE Section	Office of the Vice Chancellor
Publication Status	Final
Published Date	21 December 2022
Last Review Date	September 2022
Minimum Review Frequency	2-Yearly
Review Date	September 2024
UoE Identifier	0129