



University of Essex



Data Rights Policy and Procedures

Rights of Data Subjects under Data Protection Law

Author:	Data Protection Officer
Publication date:	--
Amended:	--
Review date:	--

Table of Contents

Data Rights Policy and Procedures	1
Table of Contents.....	2
1. Introduction.....	3
2. Responsibilities of Staff.....	3
3. Explanation of Data Rights	4
3.1 The Right to be Informed	4
3.2 Right of Access (also known as Data Subject Access Request or DSAR)	4
3.3 Right to Rectification	5
3.4 Right to Erasure	5
3.5 Right to Restrict Processing	7
3.6 Right to Data Portability	8
3.7 Right to Object	8
3.8 Rights in relation to Automated Decision Making and Profiling	9
4. Timescales and Fees	10
5. Refusing a Request	10
Appendix 1 - How to make a Data Rights Request (Guidance for Requestors)	12
Appendix 2 - Data Rights Procedure	13
Appendix 3 - Example Responses.....	15
Appendix 4 – Procedure where the request involves information about other individuals	16
Policy information.....	17

1. Introduction

It is important to the University that all personal data we collect are processed in compliance with Data Protection Law and in accordance with our Policies and Procedures. We expect all staff to follow these policies and demonstrate a commitment to protecting others' privacy.

The UK General Data Protection Regulations (UK GDPR) provide the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

In most cases the University cannot charge a fee to an individual exercising their rights.

2. Responsibilities of Staff

In order to ensure the University meets its data protection obligations we require staff to report all requests from a data subject (student/staff member or other individual) to the Data Protection Officer (dataprotectionofficer@essex.ac.uk). Staff should not attempt to respond to a request themselves.

Staff should be aware that data subjects are entitled to these rights and should ensure they follow the University's policies, procedures and codes of conduct when making records. It is important to be mindful that data subjects have a right to see what is written about them, and to challenge or change this if it is inaccurate.

3. Explanation of Data Rights

3.1 The Right to be Informed

The right to be informed covers some of the key transparency requirements of UK GDPR. It is about providing individuals with clear and concise information about what we do with their personal data.

The University complies with this right by informing individuals (at the point when we collect or obtain their information) about how we will use their personal data and what we will use them for. This information is set out in our Privacy Policies which can be found on our [privacy hub](#).

3.2 Right of Access (also known as Data Subject Access Request or DSAR)

The right of access, commonly referred to as a Data Subject Access Request, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why the University is using their data and what data we hold about them.

Certain information is exempt from the right of access; this includes:

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege
- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, judicial independence and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest

- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks
- Other exemptions which are set out on the [ICO website](#)

If the information requested contains personal data of another third party the University will consider whether it is possible to comply with the request without disclosing information that identifies another individual. The University will redact information relating to any third party; except where the other individual consents to the disclosure, or it is reasonable to comply with the request without that individual's consent.

The University will make it clear whether we have included the information about a third party and will keep records of any decisions to disclose or withhold information.

3.3 Right to Rectification

Individuals have the right to have inaccurate personal data rectified. This may involve providing a supplementary statement to incomplete data. The University can refuse this right under certain exemptions.

In some cases, the data subject may be disputing an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, the University may not be required to rectify the data.

3.4 Right to Erasure

Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right only applies to data held by the University at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances.

Individuals have the right to have personal data erased if:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed;
- consent was the lawful basis for holding the data, and you withdraw your consent;
- legitimate interests were the basis for processing, and you object to the processing of your data, and there is no overriding legitimate interest to continue this processing;
- the personal data were processed for direct marketing purposes, and you object to that processing;
- personal data were processed unlawfully;
- the data must be erased to comply with a legal obligation; or
- the personal data were processed to offer online or web services to a child.

The University will tell other organisations about the erasure of personal data where:

- the personal data have been disclosed to others; or
- the personal data have been made public in an online environment (for example on forums or websites).

The University will contact each recipient and inform them of the erasure unless this proves impossible or involves disproportionate effort.

Where a valid erasure request is received then we will take steps to ensure the erasure from backup systems as well as live systems. Those steps will depend on our retention schedule (particularly in the context of its backups), and the technical mechanisms that are available to us. It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten. Our priority is to put the backup data 'beyond use', even if it cannot be immediately overwritten.

The right to erasure does not apply where it is necessary to process the data:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;

- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to make impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise, or defence of legal claims.

If the request relates to sensitive “special category data”, e.g., about health or ethnicity then the right to erasure will not apply if:

- the processing is necessary for public health purposes in the public interest; or
- the processing is necessary for health or social care purposes and processed under the responsibility of, e.g., a health professional under a legal obligation of secrecy.

3.5 Right to Restrict Processing

Individuals have the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way the University uses their data. This is an alternative to requesting the erasure of data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information the University holds about them or how the University is processing their data. In most cases the University will not be required to restrict an individual’s personal data indefinitely; the restriction will require a time limit.

Individuals have the right to request that the processing of their personal data is restricted in the following circumstances:

- the individual contests the accuracy of their personal data and the University is in the process of verifying the accuracy of the data;
- the data has been unlawfully processed (i.e., in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead;

- we no longer need the personal data but the individual needs the University to keep the information in order to establish, exercise or defend a legal claim;
- the individual has objected to the University processing their data and we are considering whether the legitimate interests of the University override the interest of the individual;
- if an individual has challenged the accuracy of their data and asked the University to rectify it, they also have a right to request we restrict processing while we consider their rectification request;
- if an individual exercises their right to object, they also have a right to request we restrict processing while we consider their objection request.

3.6 Right to Data Portability

The right to data portability gives individuals the right to receive personal data they have provided to the University in a structured, commonly used and machine-readable format. It also gives them the right to request that the University transmits these data directly to another organisation (data controller).

The right to data portability only applies when:

- The University's lawful basis for processing this information is consent or for the performance of a contract; and
- the University is carrying out the processing by automated means (i.e., excluding paper files).

Information is only within the scope of the right to data portability if it comprises the personal data of the individual that they have provided to us.

3.7 Right to Object

Data Protection Law gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent the University from processing their personal data.

Individuals have the absolute right to object to the processing of their personal data if this is being done for direct marketing purposes.

Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in the University; or
- legitimate interests (of the University or those of a third party).

In these circumstances the right to object is not absolute.

Where the University is processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

3.8 Rights in relation to Automated Decision Making and Profiling

Automated individual decision-making is a decision made by automated means without any human involvement. This could include, for example:

- automatic acceptance onto a program of study; or
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Profiling is defined as: “Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”¹

If the University undertakes any automated decision making or profiling, we will ensure gives individuals are given the opportunity to challenge and request a review of the decision.

¹ General Data Protection Regulations, Article 4(4)

4. Timescales and Fees

The University has a legal obligation to comply with a request without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of:

- any information required to confirm the requester's identity; or
- a fee (if charged) in exceptional circumstances.

The University will calculate the time limit from the day we receive the request (whether it is a working day or not) until the corresponding calendar date in the next month. We can extend the time to respond by a further two months if the request is complex or we have received several requests from the same individual. The University will let the individual know within one month of receiving their request and explain why the extension is necessary.

5. Refusing a Request

Data Protection law provides certain exemptions under which the University is not required to comply with a request. If an exemption applies, the University can refuse to comply with a request wholly or in part. The ICO has detailed guidance on [Exemptions](#) which the University will follow when applying an exemption. The University is committed to considering each request on a case-by-case basis.

The University can also refuse to comply with a request if it is:

- manifestly unfounded; or
- excessive; or
- the identify of the data subject (and/or a third party acting on their behalf) has not been verified

In cases where the request is manifestly unfounded or excessive, the University may alternatively consider charging a fee under these circumstances.

The University will inform the individual without undue delay and within one month of receipt of the request if we are refusing the request. We will provide the following information in the refusal notice:

- the reasons we are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

We will also provide this information if we request a reasonable fee or need additional information to identify the individual.

Appendix 1 - How to make a Data Rights Request (Guidance for Requestors)

You can make a request verbally or in writing, including on social media. A request is valid if it is clear that you are asking for your own personal data. You do not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

You may also ask a third party (e.g., a relative, friend or solicitor) to make a request on your behalf. Before responding, the University needs to be satisfied that the third-party making the request is entitled to act on your behalf and we may ask for documents to evidence this.

In order to facilitate the management of data rights requests we would normally advise individuals to submit a request via the following process:

1. Making a Data Rights Request

Please complete the form [Data Subject Access Request](#) or email the Data Protection Officer dataprotectionofficer@essex.ac.uk providing:


- your name
- relationship to the university (i.e., student, staff, applicant etc)
- the right you wish to exercise e.g., right of access, or data to be erased etc.
- any other information that will assist us in locating the personal data.


2. Proof of identity

If we have doubts about your identity when making the request, or if a third party organisation makes the request on your behalf, we will ask for more information to confirm who you are and/or the authority under which the third party is acting on your behalf.

We will let you know without undue delay and within one month if we need more information from you to confirm your identity. We will comply with the request once we have received the additional information.

Appendix 2 - Data Rights Procedure

 Request received (by member of staff within the University) or directly through webform

 Forward to the Information Assurance Team as soon as received
(dataprotectionofficer@essex.ac.uk)

Information Assurance Team will record the details on internal system including data received, date due and information required/exercise of specific right



Confirm ID and/or entitlement:

The Information Assurance Team may ask the applicant to provide copies of ID documents (Passport, Driving Licence, Utility Bill [from last 3 months]) if they need to verify the identity of the requestor. The Information Assurance Team may need to ask for evidence of entitlement where the request is made by a third party. If this documentation is required, the clock will stop on the timescale for compliance until it is received.



Clarify scope of request:

The Information Assurance Team will contact the requestor if clarification is required to identify the specific the information requested or right being exercised. If clarification is required, the clock will stop on the timescale for compliance.



Information Assurance Team will contact relevant departments asking them to supply the information (providing a link to a secure storage area) or asking for them to support the fulfilment of a data right e.g., to provide copies of records, restrict processing or erase data



Information Assurance Team will provide the information or confirm the right has/has not been complied with. The request will then be closed on the internal system.

Appendix 3 - Example Responses

Acknowledgement

Dear [name of requestor]

Reference: XXXXX

We acknowledge receipt of your request received on [date] [by email/via the website form...] and are handling this as a Data Subject Access Request under the Data Protection Act 2018. In order to progress your request, we need to check your identity [set out process]. Once we are satisfied, we then have one calendar month in order to respond to your request. [Set out any other relevant details].

Response

Dear [name of requestor]

Reference: XXXXX

[Please find attached the information you requested]

[Please be advised that we have/have not complied with your [specific request]. [We have not complied with your request because [explanation].

We hope that we have responded satisfactorily to your request. If you are not satisfied with our response, you should contact us to review a review, if following our review, you are still not satisfied you have the right to contact the Information Commissioners Office (ICO). They can be contacted at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK95AF (<https://ico.org.uk/>)

Please remember to quote the reference number above in any future correspondence about this request.

Appendix 4 – Procedure where the request involves information about other individuals

Personal data can relate to more than one person. Therefore, responding to a DSAR may involve providing information that relates to both the requester and another individual.

As a general guide the University will:

- Redact the personal details of any student (who is not the data subject);
- Redact the personal details of employee's except where:
 - The personal detail of an employee was disclosed to the data subject as part of direct correspondence with the data subject e.g a letter or email signature;
 - The personal details relate to the minutes of a meeting which the data subject attended e.g. names of the attendees included in the minutes
- Redact the personal details of any third party (who is not a student or an employee);

It is important to note that these are a general guide and the University will always follow the text of the legislation or relevant guidance published by the Information Commissioner's Office.

The data subject may also ask for clarification as to the reason for the redaction, at which point the University may reconsider whether the third party data can be disclosed. If this is the case the University will either seek the consent of the third party or consider whether it would be reasonable to comply with the request without the third party individual's consent.

Policy information

Title: Data Rights Policy

Policy Repository Identifier: 0127

Policy Classification: Policy

Security Classification: Open

Nominated Contact: dataprotectionofficer@essex.ac.uk

Policy Manager Role: Data Protection Officer

Policy Owner Role: Deputy University Secretary

Responsible UoE Team: Information Assurance Team

Responsible UoE Section: Office of the Vice-Chancellor

Publication Status: Final

Published Date: April 2022

Last Review Date: April 2022

Minimum Review Frequency: 2-Yearly

Review Date: April 2024