University of Essex

Appropriate Policy Document

As required under Data Protection Law

Authors:	Data Protection Officer
Publication date:	June 2024
Amended:	June 2024
Review date:	June 2026

Table of Contents

Appropriate Policy Document 3

1. Introduction 3

2. Description of data processed 3

3. Conditions for processing special category and criminal offence data 5

4. Compliance with the Data Protection Principles 6

5. References 8

Appropriate Policy Document

1. Introduction

This policy has been developed by the University of Essex to meet the requirement under Data Protection law for an Appropriate Policy Document (APD). This details the lawful bases and conditions for processing, and the safeguards the University has put in place, when processing special category personal data and criminal offence data.

Special category personal data is defined at Article 9 of the UK General Data Protection Regulations (GDPR) as:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- 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

Data Protection law also has specific provisions relating to the processing of criminal offence data.

The University is allowed to process these data under data protection law but some of the conditions for processing special category and criminal offence data require us to have an APD in place.

The University processes special category personal data in other instances where it is not a requirement to keep an APD. The processing of such data respects the rights and interests of the data subjects. Clear and transparent information about why the University processes personal data (including the lawful basis for processing) is set out in the University’s privacy notices.

2. Description of data processed

The University processes special category personal data in the following circumstances.

2.1 As an employer

Special category data about employees are processed because it is necessary to fulfil the University's obligations as an employer. This includes information about our employees':

- health, for the following purposes:
    - to discharge our health and safety obligations
    - to determine our employees are fit to work
    - to handle staff sickness and absence records
    - to support employee wellbeing, including in order to make any necessary adjustments for disability, such as accessibility alterations to our facilities and facilitating any additional needs such as library access.
- ethnicity and sexual orientation (in relation to our equal opportunities monitoring); and
- membership of any trade union (for taking payroll deductions only)

Further information about this processing can be found in the University's staff privacy notice.

2.2 As a place of study

Special category data about students and applicants to the University are processed. This includes information in relation to their:

- health and wellbeing (in order to provide support in relation to their health and wellbeing, including in order to make any necessary adjustments for disability, such as accessibility alterations to our facilities); and
- ethnicity and sexual orientation (in order to monitor compliance with equality legislation).

Further information about this processing can be found in the University's student privacy notice.

2.3 Criminal convictions processing

- The University also processes criminal offence data under Article 10 of the GDPR. As an employer, the University processes criminal offence data in relation to pre-employment checks and declarations by an employee or prospective employee (in certain roles).
- As a place of study, the University processes criminal offence data in relation to courses where a DBS check is required, or where the University Student Membership and Disclosure and Barring Service Check Policy deems one is necessary.

3. Conditions for processing special category and criminal offence data

The University processes special categories of personal data under the following GDPR Articles:

- Article 9(2)(b) – processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the University or the data subject in connection with employment, social security, or social protection (e.g., the processing of employee sickness/absence records and processing required to ensure employees are fit to work). The University relies upon the corresponding provision in the Data Protection Act 2018 (Schedule 1, Part 1, Paragraph 1 (Employment, social security, and social protection)) for this processing activity
- Article 9(2)(g) – reasons of substantial public interest (e.g., processing data to ensure equality of opportunity or treatment of students, applicants, and employees). The University relies upon the corresponding provision in the Data Protection Act 2018 (Schedule 1, Part 2, Paragraph 8 (Equality of Opportunity or Treatment)) for this processing activity
- Article 9(2)(i) – processing is necessary for reasons of public interest in the area of public health (e.g., processing relating to responding to new threats to public health (e.g., epidemics, pandemics or new research findings)

The University processes special category and criminal offence data under the following paragraphs of Part 1 and Part 2 of Schedule 1 of the Data Protection Act 2018:

- Part 1: Paragraph 1 (Employment, social security, and social protection)
- Part 1: Paragraph 2 (Health or social care)
- Part 1: Paragraph 3 (Public health)
- Part 1: Paragraph 4 (Research)
- Part 2: Paragraph 5 (Substantial Public Interest Conditions)
- Part 2: Paragraph 6(1) and (2)(a) (Statutory and government purposes)
- Part 2: Paragraph 8 (Equality of opportunity or treatment)
- Part 2: Paragraph 9 (Racial and ethnic diversity at senior levels of organisations)
- Part 2: Paragraph 10 (Preventing or detecting unlawful acts)
- Part 2: Paragraph 11 (Protecting the public against dishonesty etc
- Part 2: Paragraph 12 (Regulatory requirements relating to unlawful acts and dishonesty

- Part 2: Paragraph 14 (Preventing fraud)
- Part 2: Paragraph 17 (Counselling)
- Part 2: Paragraph 18 (Safeguarding of children and of individuals at risk)
- Part 2: Paragraph 20 (Insurance)
- Part 2: Paragraph 21 (Occupational pensions)
- Part 2: Paragraph 24 (Disclosure to elected representatives)

4. Compliance with the Data Protection Principles

In this section, the University sets out how it complies with each of the data protection principles. The University has put in place appropriate technical and organisational measures to meet the requirements of the GDPR and Data Protection Act 2018. These include:

4.1 Accountability Principle

The University complies with the accountability principle under the GDPR, including taking the following steps:

- appointing a designated data protection officer role which may report directly to the highest management level
- taking a ‘data protection by design and default’ approach to the University’s activities
- maintaining documentation (ROPAs) of processing activities
- adopting and implementing data protection policies
- ensuring the University has written contracts in place with data processors
- implementing appropriate security measures in relation to personal data processed
- carrying out data protection impact assessments (DPIAs) for high-risk processing and
- reviewing and updating the University accountability measures regularly, or amending when required

4.2 Principle (a): lawfulness, fairness and transparency

The University will only process personal data where it is lawful, and the University has been fair and transparent.

The University provides clear and transparent information about why personal data are processed including the lawful basis for processing in the University's privacy notices, which can be found on our privacy hub.

The University can only process personal data where we have a lawful basis for doing so under Article 6 of the GDPR and where we provide transparency around our legal bases. Where the University processes special categories of personal data, or criminal records data, we need an additional legal basis to rely upon, as set out above in this APD and in our privacy notices.

Processing for purposes of substantial public interest is necessary for the exercise of the functions of a Higher Education Institution and exempt charity under the Charities Act 2011.

4.3 Principle (b): purpose limitation

Personal data are processed only for specified, explicit and legitimate purposes. They must not be further processed in any manner incompatible with those purposes.

We will only collect personal data for specified purposes and will inform data subjects what those purposes are through our privacy notices.

The University processes personal data for purposes of substantial public interest (as explained above) when the processing is necessary for the University to fulfil its statutory functions.

Where the University is sharing data with another data controller, the University will document that we are authorised by law to process the data for that purpose.

The University will not process personal data for purposes incompatible with the original purpose for which they were collected.

4.4 Principle (c): data minimisation

The University will only collect personal data necessary for the relevant purposes and ensure this collection is not excessive.

The information the University processes is necessary for and proportionate to its purposes.

Where personal data are provided to or obtained by the University, but are not relevant to the University purposes, they will be erased.

4.5 Principle (d): accuracy

Where personal data are inaccurate or out of date, having regard to the purpose for which they are being processed, the University will take every reasonable step to ensure that data are erased or rectified without delay.

Where the University decides not to either erase or rectify data, for example because the lawful basis relied upon to process the data means these rights don't apply, this decision will be documented.

4.6 Principle (e): storage limitation

All special category data processed by the University, unless retained longer for archiving purposes, are retained for the periods set out in the University's retention schedules.

The University determines the retention period for data based on legal obligations, industry best practice and the necessity of its retention for business needs.

The University retention schedule is reviewed regularly and updated when necessary.

4.7 Principle (f): security, integrity and confidentiality

Electronic information is processed within the University's secure networks.

Hard copy information is processed in line with policies and procedures for data protection and information security.

The University's electronic systems and physical storage have appropriate access controls applied.

The systems the University uses to process personal data allow the erasure or updating of personal data where appropriate.

5. References

This Policy has been based on the ICO Appropriate Policy Document and HMRC Appropriate Policy Document and has been produced under the Open Government Licence

- ICO Appropriate Policy Document
- HRMC Appropriate Policy Document

Document Control Panel

Field	Description
Title	Appropriate Policy Document
Policy Classification	Policy
Security Classification	Open
Security Rationale	None
Policy Manager Role	Data Protection Officer
Nominated Contact	dataprotectionofficer@essex.ac.uk
Responsible UoE Section	Office of the Vice-Chancellor
Approval Body	University Steering Group
Signed Off Date	August 2024
Publication Status	Published
Published Date	August 2024
Last Review Date	June 2024
Minimum Review Frequency	2-Yearly
Review Date	June 2026
UoE Identifier	0156

If you require this document in an alternative format, such as braille, please contact the nominated contact at dataprotectionofficer@essex.ac.uk.