Assurance & Data Protection Office Privacy Notice

How we use your data

This Privacy Notice outlines how the Assurance and Data Protection Office at the University of Kent collects, uses and manages the personal information of individuals in accordance with data protection law.

The University of Kent is registered as a 'Data Controller' under registration number Z6847902. View the full entry on the register

How we collect your personal information

Your personal data is obtained:

- directly from you, through online or paper forms, email or by telephone
- from your parents if they are permitted, either legally due to your age or after you have given your consent
- from other departments at the University
- from police or other law enforcement authority, e.g. when they are making a request for information about a student or staff member
- from online checking tools where we assist teams with sanctions or export control checks, or
- from your Solicitor or from the courts or Tribunals in relation to legal claims or proceedings.

Categories of information we collect

Personal data we collect about you in connection with Data Rights requests, Freedom of Information requests and Police requests, or in order to provide the wider assurance functions:

- name
- address / postcode
- telephone number
- email address
- date of birth
- Identification number (e.g. NI, Passport, student / employee number)
- student / staff record
- student / employment references
- your opinions and opinions recorded about you by others
- your reasons for contacting us (details of your request, complaint or enquiry)
- your image (in relation to CCTV footage or photographs)

- any information included in public sanctions lists compiled by HM government the EU or OFAC (US)
- details of any assurance, legal compliance query, claim or proceedings involving you.

Special category data we collect about you in connection with Data Rights requests, data incident investigations and police requests, and in relation to internal assurance and legal advice where applicable:

- biometric data for uniquely identifying you
- physical or mental health data
- racial or ethnic origin
- sex life or sexual orientation
- religious or philosophical beliefs
- political opinions
- trade union membership.

Criminal offence data we collect about you in connection with Data Rights requests, data incident investigations and police requests, and in relation to internal assurance and legal advice where applicable**:**

- allegations that someone has committed a criminal offence
- actual offence or criminal record information
- criminal court proceedings or sentencing data.

How we use your personal information

We will use your information in the following ways:

- to comply with EU or UK General Data Protection Regulation (GDPR) information rights requests,
- to comply with obligations under the Freedom of Information Act 2000 (FOIA) the Environmental Information Regulations 2004 (EIR) when processing requests

This will include establishing whether the request is valid; locating, retrieving and collating information relevant to your request, consulting individuals (for example University staff and third parties) affected by your request, identifying whether any information is available to you and whether any information should be validly withheld from disclosure; preparing and sending the response to your requests, review requests or appeals to the Information Commissioner's Office (ICO).

- to meet the requirements around breach management and notification contained within the EU and UK GDPR
- to help the university comply with its legal obligations, or
- to advise and assist staff by providing advice in relation to complaints, agreements, legal advice or litigation, or in relation to risk, ethics, or fraud matters.

If a data subject or law enforcement body does not provide sufficient personal data to us to allow us to verify the identity of a data subject, we may not be able to process the information request.

If a FOI requestor does not provide their real name and include an address for correspondence, the FOI Request may not be valid (in accordance with Section 8 of the Freedom of Information Act) and as such we may not be able to process the information request.

If we are not provided with personal data that has been involved in a data incident, we may not be able to inform affected data subjects (where necessary) and/or assess the risk posed by the incident to the affected individual(s).

Our lawful basis for processing your data

We rely on the following lawful basis as allowed by the UK GDPR for processing your personal data as this is necessary for:

- a legal obligation – Article 6(1)(c), i.e. to comply with data rights requests and to meet the requirements around data breach management and notification, under UK GDPR; to comply with obligations under FOIA when processing requests and to comply with any regulatory reporting requirements associated with the assurance function (such as under the Sanctions and Money Laundering Act 2018, the Export Control Act 2002)

- for the performance of tasks carried out in the public interest – Article 6(1)(e), i.e. as associated with the University's functions as a public authority and higher education institution when providing internal advice to departments or when sharing information with law enforcement.

- Legitimate interests of the University or a third party – Article 6(1)(f) (where necessary to process your data for the purposes of the University's or a third party's legitimate interests. We will carry out a legitimate interests test to ensure that there is a legitimate public interest in disclosure that is necessary to meet the public interest and which does not cause unwarranted harm to you as an individual.

As we also use your special category data, we must identify a further basis for processing that data. The processing is necessary:

- for substantial public interest reasons (complying with statutory requirements, for preventing or detecting unlawful acts, protecting the public against dishonesty, regulatory requirements, safeguarding or fraud purposes) – Article 9(2)(g)

- to protect your vital interests or those of another where you are physically or legally incapable of giving consent – Article 9(2)(c)

- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity – Article 9(2)(f).

As we also use your criminal offence data, we additionally rely on the following conditions (where applicable) from *Schedule 1, Part 3* of the Data Protection Act 2018*:*

- 30(a) the processing is necessary to protect the vital interests of an individual
- 30(b) the data subject is physically or legally incapable of giving consent
- 33(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)
- 33(b) is necessary for the purpose of obtaining legal advice
- 33(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights, or
- 36 the extension of conditions referring to substantial public interest (complying with statutory requirements, preventing or detecting unlawful acts, protecting the public against dishonesty, safeguarding or fraud purposes).

We have a Special Category and Criminal Offence Data Appropriate Policy document in place throughout the time that we use your data and for 6 months after we cease to use it.

The legal obligations include those set out in:

- the Freedom of Information Act 2000
- the Environmental Information Regulations 2004
- the Regulation (EU) 2016/679 (known as EU GDPR)
- the Data Protection Act 2018
- the Sanctions and Money Laundering Act 2018 and associated regulations
- the retained EU law version of the GDPR by virtue of section 3 of the EU (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) regulations 2019 (known as UK GDPR).

Who your information will be shared with

We will share details of the request with members of staff who hold the information requested or who are asked to contribute to the University's response. In relation to FOI/EIR requests from journalists or media organisations we will share responses with members of our communications team. Generally, for FOI/EIR requests we will remove the names of requestors before forwarding the request to the staff who hold the information.

We use third party organisations (known as data processors) who carry out services on the University's behalf under contract. We will ensure that only the minimum

amount of relevant personal data necessary for the purpose is transferred. We will ensure that contractual agreements exist to ensure compliance with data protection regulations and that data is used solely under our instruction. In these circumstances personal data shall be deleted after the contract has terminated.

- *Microsoft*
- *Digital Interactive Ltd who provide our case management software system Infreemation*

Sometimes it is necessary for your personal information to be shared:

- with competent authorities (such as the police, NCA, the ICO) or action fraud for law enforcement purposes or for regulatory reporting purposes (central government departments such as OFSI or the ECJU) (for substantial public interest reasons)
- the ICO or Tribunal if you have made a complaint
- with insurers to support claims
- with third parties (if relevant we will share the details of the request with your name redacted for example if the request relates to information held in confidence.)
- with our professional advisors or with courts and Tribunals where it is necessary for the establishment, exercise or defence of legal claims.

Occasionally the University may, if appropriate, legitimate and necessary, rely on relevant exemptions to UK GDPR provisions as are allowed under the Data Protection Act 2018 (in relation to crime and taxation, management forecasts, negotiations, confidential references, exam scripts and exam marks and legal professional privilege).

Transfer of your information outside of the UK

When it is necessary for us to transfer your personal information across national boundaries, we will ensure this safeguards your personal information by requiring such transfers are made in compliance with all relevant data protection laws. This will only apply when an information request is received from a competent authority based overseas, for example, a law enforcement authority.

We will ensure the transfer is authorised by:

- adequacy regulations made by the Secretary of State found here International transfers: a guide | ICO
- safeguards prescribed by the UK GDPR, guidance for which can be obtained from the ICO website: International transfers: a guide | ICO

Microsoft's standard contractual clauses can be viewed here. Digital Interactive Ltd's dedicated servers for our Infreemation case management system are UK based and no data is kept outside the UK.

How long your personal data will be kept

- For Data Rights Requests: Last action + 6 years
- For Data Breaches and mitigations: Last action + 6 years
- For Police Requests for data: Last action + 6 years.
- For FOI requests: Last action + 6 years
- For assurance and legal advice matters: Last case action + 6 years.

Security

We will ensure that security measures are in place to prevent the accidental loss, unauthorised use or access to your data. Access is given to staff on a 'need to know' basis. Our staff are required to keep your data safe and complete data protection training.

We have procedures in place to deal with any data security incidents and will notify you and the ICO in the event of a data breach where we are required to do so.

Your rights

Please be aware of the following rights which can be accessed free of charge by contacting dataprotection@kent.ac.uk:

- know how we are using your personal information and why (right to information)
- access the personal data held by us (subject access request)
- ask for correction of any mistakes (rectification)
- to object to direct marketing
- to complain to the ICO

In some circumstances you also have the right to:

- object to how we are using your information
- ask us to delete information about you (the right to be forgotten)
- have your information transferred electronically (data portability)
- object to automated decisions which significantly affect you
- restrict us from using your information.

For further guidance regarding your rights please see the ICO website.

Your rights- if you have given consent or explicit consent for a specific use of your personal data

You can withdraw your consent at any time.

You can do this by contacting us at: dataprotection@kent.ac.uk

This does not affect the lawfulness of the processing based on consent before its withdrawal.

Your right to complain to the Information Commissioner

You have the right to lodge a complaint with the Information Commissioner's Office.

The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Website: ico.org.uk

Their helpline telephone number is: 0303 123 1113.

Contacts

If you have any questions or concerns about the way the University has used your data, or wish to exercise any of your rights, please consult our website.

The University's Data Protection Officer can be contacted at:
dataprotection@kent.ac.uk

Assurance and Data Protection
The Registry
The University of Kent
Canterbury CT2 7NZ

Document review date

This privacy notice will be reviewed at least annually.

Version	Author	Description of Change	Date	Next Review date
1.0	Assurance and Data Protection Team	Final version	06/12/2022	06/12/2023
2.0	Assurance and Data Protection Team	Review to add new case management provider, legitimate interests basis	05/10/2024	05/10/2025