Privacy Notice – Student Engagement

How we use your data

This Privacy Notice outlines how Student Engagement 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 hardship funding applications and extenuating circumstances requests.
- from your central student record (please see the student enrolment privacy notice for further information).
- from attendance and engagement data (including registrations of attendance at teaching activities, and submissions and activity on Moodle).
- from your academic department, or other parts of the University, such as campus security.
- from other third parties (such as parents, guardians and friends if they report safeguarding concerns to us).
- when we create records such as of meeting notes relating to any meeting between you and Student Engagement staff.

Categories of information we collect

Personal data we collect about you in connection with the work carried out by Student Engagement team.

- your name, address and postcode.
- telephone numbers.
- email addresses.
- date of birth.
- gender and pronouns.
- student identification number.
- course of study and school.
- information regarding affiliations (for example, with student societies, residence associations, and other group memberships).
- visa and enrolment status.
- details of any issues, incidents, or personal circumstances that may require support or risk management (as reported by you or by a third party).
- disciplinary issues (where relevant to disciplinary panel or decision making).
- financial information (related to support fund or bursary applications).

Special category data we will collect about you in connection with meeting our equalities monitoring obligations, supporting the provision of a reasonable adjustment or providing financial support (if relevant)

- racial or ethnic origin.
- physical or mental health data (including access requirements, and all information included in Inclusive Learning plans).

Criminal offence data:

We receive incident reports from campus security and concerns from third parties which may contain details that include allegations that an individual has committed a criminal offence.

How we use your personal information

Our objective is to ensure an excellent educational experience both curricular and extra curricular whilst protecting your privacy by abiding by data protection law.

We will use your information in the following ways:

- for student welfare support purposes.
- to facilitate support for students.
- to respond to security incidents relating to students, staff or members of the community.
- to respond to complaints or issues raised by students, staff or members of the community.
- when we are asked to be a member of a disciplinary, support to study, fitness to practice, or other panel.
- for safeguarding purposes
- to make reasonable adjustments to support teaching and learning.
- to facilitate and assess funding/bursary/scholarship applications
- to assist the data protection team with statutory requests for information
- to conduct data analysis and reporting (using pseudonymised information) to understand student support needs, and where targeted support or intervention may be required.
- for collating statistical information about our service (using pseudonymised information), for the purpose of service improvement and audits
- for equalities monitoring purposes.
- to track the progress of student cases and monitor the individual support offered by the team.

As we have a statutory basis to process your personal data if we do not receive this information, in some cases we may not be able to provide you with relevant support services.

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:

- the performance of a task carried out in the public interest -Article 6(1)(e) as part of our role of being a teaching and research institution and meeting our obligations to support you;
- a legal obligation – Article 6(1)(c) (such as under the Equality Act 2010, Freedom of Information Act 2000 or as required by a court order)
- to protect your vital interests or those of another person – Article 6 (1)(d) (where we need to process information about you in an emergency)
- you have given your consent for one or more specific purposes- Article 6(1)(a) (for example to disclose sensitive information about you as part of a specific funding application)

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

- employment, social security and social protection – Article 9(2)(b)
- to protect your vital interests or those of another where you are physically or legally incapable of giving consent – Article 9(2)(c)
- you have manifestly made the data public – Article 9(2)(e)
- us to establish, exercise or defend legal claims (or where courts are acting in their judicial capacity) – Article 9(2)(f)
- reasons of substantial public interest (as defined within the Data Protection Act 2018)– Article 9(2)(g).

Our substantial public interest reason(s) is/are:

    - statutory purposes
    - equality of opportunity or treatment
    - safeguarding
    - prevention or detection of crime

- statistical purposes with a basis in law - Article 9(2)(j) (we will ensure that Article 89(1) UKGDPR and section 19 DPA 18 are satisfied – we will apply appropriate safeguards by minimising the personal data and pseudonymising any data used for the purposes of data analysis and reporting)
- where you have given your explicit consent -Article 9(2)(a)

As we also use your criminal offence data, we additionally rely on the following conditions in Schedule 1 of the Data Protection Act 2018: consent (for vetting); vital interests (in an emergency); information in the public domain (if relevant to a complaint or serious incident); in relation to legal claims or judicial acts (such as court orders); or for substantial public reasons as mentioned above (safeguarding, prevention of crime etc).

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.

Who your information will be shared with

We may share information internally to other university departments where necessary (for example when you make an application for funding, or if there is a safeguarding concern).

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 is a data processor for the University's personal data, because we use Microsoft 365 to store files and emails. We also use:

- Target Connect software for our case management system, supplied by GTI Futures Ltd
- Blackbullion Ltd software for processing hardship applications
- Presto Student attendance monitoring software provided by Simac IDS Ltd.

We share your personal data with third party data controllers for their legitimate purposes (such as courts or the emergency services). In some cases we are required by law to share information with external organisations.

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

- with competent authorities (such as the police, NCA) or action fraud for law enforcement purposes (for on substantial public interest reasons – Article 9(2)(g) – for preventing or detecting unlawful acts, safeguarding or fraud purposes.
- with our professional advisors where it is necessary for the establishment, exercise or defence of legal claims – Article 9(2)(f).

Very 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 and exam scripts and exam marks).

Transfer of your information outside of the UK

When it is necessary for us to transfer your personal information across national boundaries to a third party data processor, such as one of our service providers, we will ensure this safeguards your personal information by requiring such transfers are made in compliance with all relevant data protection laws.

Microsoft store personal data locally. Details of the safeguards in place for any authorised transfers can be found on their website in their Data Protection Addendum.

GTI Futures Ltd (Target Connect) process data in the UK. Blackbullion Ltd and IDS Ltd process data within the EEA. Any transfer within the EEA is authorised by adequacy regulations made by the Secretary of State listed on the DCMS website.

How long your personal data will be kept

Please see our Document Retention and Archiving Policy for details on how long the University keeps your core student records.

In Student Services we keep most records for 6 years from the date you left the University.

If the records relate to a fund or bursary application we keep these for 6 years from the date of the grant or for 1 year if your application is unsuccessful. In relation to the Gender Affirmation Fund we keep information of all applications after which only the Student ID number is kept for the duration of your time with us (up to 4 years).

User data within our attendance monitoring system is kept for 1 academic year.

We also store legacy records relating to our Covid reporting requirements for 6 years from the date of report.

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
- information about the existence of automated decision-making (including profiling) and meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for you, and in some cases to object to the decisions made
- 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 HeadofStudentEngagement@kent.ac.uk with your request to remove consent.

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.

Their helpline telephone number is: 0303 123 1113.

Your obligations

The University tries to ensure that the information it holds is accurate and up-to-date. It must, however, rely on students to inform the appropriate office of any change in their personal data. In particular, any change of home or term-time address should be notified to the Central Student Administration or online via the Student Portal.

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

Document review date

This privacy notice will be reviewed at least biennially.

Version	Author	Description of Change	Date	Next Review date
1	Head of Student Engagement	Adapted from Student Services Privacy Notice	20/08/24	
1.1				