

Privacy Notice

How we use your data

This Privacy Notice outlines how the Department of Human Resources and Occupational Development at the University of Kent collects, uses and manages the personal information of individuals using the Report+Support or directly to the University 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.

The privacy information is specific to the processing of the personal data collected via the Report+Support [online tool](#) and should be read in line with the University's main [Privacy Notice](#).

How we collect your personal information

The Report + Support tool provides staff with a portal to report and/or seek assistance in matters of inappropriate and unwanted behaviours of others on campus.

Your personal data is obtained:

- directly from you, through the online Report + Support form
- from others, who provide reports to us (although they may choose not to give their name when doing so).

Categories of information we collect

Personal data we collect about you in connection with the provision of staff support and to process staff disciplinary cases under the Sexual Violence and Misconduct Policy and Respect at Kent Policies and Procedures via the Report + Support online service.

When you use the portal to make a report, you will be providing:

- Your name.
- Your work based contact details (email and telephone number).
- Employment Status with the University.
- your division (if provided when reporting a concern).
- Information about third parties who are involved which may identify them.
- Your own additional free text information (optional) which includes special category data and specific characteristics (about you) that you consider relevant to your report (such as age, being trans/nonbinary, having caring

responsibilities, disability, gender, having children/pregnancy, ethnicity, nationality, religion, sexual identity or other special category data as identified below).

As a result of reporting via the portal and in using the Report + Support service, where appropriate (and normally in consultation with you) reports may be shared with relevant colleagues within HR services or student services.

Any data used for statistical purposes will be fully anonymised to protect confidentiality.

- On certain rare occasions where there is a high risk to safety or evidence of suspected criminal activity/behaviour, the University may be duty bound to take action immediately without your consent.

How we use your personal information

When processing personal data of students, staff and others, we will try to ensure that we consider the rights and freedoms of all concerned

Anonymous disclosure: Where an anonymous disclosure is made, the University will not be able to identify the person who made the disclosure. However, if other parties are named, or sufficient details are provided then the University may be able to identify those individuals. The University will review those details when reviewing portal reports and may decide that further investigation is necessary, under its duty of care. The University will also use data gathered via anonymous disclosures to produce statistics and management reports – those will be used by the University to identify where actions are necessary to improve and/or strengthen the safety, wellbeing of our students, staff and wider community.

Named disclosures: When you provide your name, the University will contact you and/or any named third parties to seek any further information that may be needed, or to provide support and/or to discuss possible options. The University will use the details of third parties identified in a disclosure to assess if there are risks to themselves or others, doing so may lead to further actions, including formal action such as a disciplinary investigation, or disclosure to the Police, of suspected criminality, where there is a reasonable belief that there is significant risk to others. Reports provided from the portal are assessed securely by a small group of authorised University staff with role based access to the portal within HR Services. It may then be necessary to further share the report with appropriate third parties such as the Police, counsellors, Divisional Faculty colleagues etc., to provide you with support and resolution.

In order to process your data, the University is required to have a purpose and legal basis to do so.

This is explained further in the next section.

Our lawful basis for processing your data

The University relies on the following lawful bases under UK GDPR and the Data Protection Act 2018 for processing your personal data.

Purposes of data Processing	Lawful basis for processing personal and/or special category data
Provision of a portal for staff support and collection of data directly provided from a staff member into the Report + Support service – your use of that portal to report an incident or matter that relates to you or someone else. You can choose to remain anonymous	UK GDPR Article 6 1(a) – consent. You have sought the use of the portal and agreed to its terms and conditions of use, providing information that you agree will help us to support you with the matter raised.
Identifying the most appropriate person or source of support in relation to the issue/concern/incident/event	UK GDPR Article 6 1 (b) - Processing is necessary for the performance of the University's contractual obligations to staff and students
<p>Reviewing a report and taking further action under relevant University policies and procedures as required i.e., supporting you, initiating an investigation, managing the disciplinary action procedure.</p> <p>Meeting our duty of care, health and safety, Equality Act 2010, safeguarding and other obligations to staff and students in the University community.</p> <p>Meeting our wider legal and regulatory obligations in the delivery of HR services for staff</p>	UK GDPR Article 6 1 (c) - Processing is required to meet legal obligations under various forms of legislation or forms part of our wider public interest tasks in creating a safe working environment
Anonymising your data for statistical and reporting purposes	UK GDPR Article 6 1 (f) – The University has a legitimate relationship to the data for anonymisation purposes

	and has a legitimate interest basis to process the data
Referral to other support services / medical intervention; the need to seek urgent medical attention or emergency service support	UK GDPR Article 6 1 (d) where processing may be necessary to meet an individual's vital interest needs. For special categories of personal data (i.e., your health or ethnicity) we rely on either your explicit consent (UK GDPR Article s 6 1 (a) and 9 2 (a) or to meet various data processing conditions in the substantial public interest (e.g., safeguarding, counselling or prevention of criminal behaviour) (UK GDPR Articles 6 1 (e) and 9 2 (h), (i))

*We will only seek to rely on the lawful basis of protecting the vital interests of you or some other individual where either you or the other individual are incapable or unable to provide consent.

Our public task and other statutory purposes are underpinned by our powers and duties as a higher education institution and include. We have legal duties as an employer to maintain compliance with the Equality Act 2010, and hold a duty of care to our employees under Health and Safety at Work Act (1974).

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

Once you have submitted a report, you cannot withdraw any of the information you have provided into the portal.

Outside of the portal and during the course of staff support, data will be shared with internal departments of the University and in these cases, access to personal data will be limited to only those who are supporting you, or who are investigating or adjudicating your report, using the minimum amount of data for the purpose required.

We use third party organisations (known as data processors) who carry out services on the University's behalf under contract. We will ensure that contractual agreements exist to ensure compliance with data protection regulations and that data is processed only under our instruction. In these circumstances personal data shall be deleted after the contract has terminated.

Personal information submitted to the Report+Support system is handled by Culture Shift, who are data processors providing the information and application on our behalf. You should also review the [Culture Shift Privacy Policy](#). Culture Shift staff may occasionally need to access the portal system to provide technical support and manage an incident response. Such access is granted on an enhanced security basis and subject to strict contractual, technical and organisational controls.

The University stores data on Microsoft servers who act as a third-party processor on our behalf.

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

- With competent authorities (such as the police, National Crime Agency) or Action Fraud for law enforcement purposes (for substantial public interest reasons – UK GDPR 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).

On very rare occasions 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).

Transfer of your information outside of the UK

When it is necessary for us to transfer your personal information across international 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.

Data will be stored electronically in the University's servers hosted by third-party (Microsoft) secure cloud services platform and ResourceLink (StaffConnect). All data is stored within the UK or EU. The transfer to the EU is permitted through:

- adequacy regulations made by the Secretary of State. Further details can be found [here](#).

How long your personal data will be kept

Personal data is kept, deleted or archived in accordance with the HR Records Retention Schedule which can be found within Schedule 2 of the [HR privacy statement](#). Staff submissions to Report+Support and Staff data relating to conduct and disciplinary proceedings are retained for 7 years following end of engagement. Anonymised information in connection with the Report+Support portal may be retained for longer to monitor and assess our work in this area.

Security

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

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

- To know how we are using your personal information and why (right to information)
- To request a copy of the personal data held by us (subject access request)
- Ask for correction of any mistakes (rectification)
- 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)
- Restrict us from using your information.

For further guidance regarding your rights please see our [Assurance and Data Protection website page on data protection rights](#) or the ICO website.

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

Information provided by you into the Report+Support portal cannot be withdrawn. However, where you have further consented to the use of your information as part of the service, you can withdraw your consent at any time.

You can do this by contacting us at the Employee Relations team in the Department of Human Resources and Organisational Development. Please email us at hremployeerelations@kent.ac.uk to request the withdrawal of your consent for data submitted via the Report+Support system to be used or by contacting the Assurance and Data Protection Team 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.

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 access rights under UK General Data Protection Regulations, 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 annually.

Version	Author	Description of Change	Date	Next Review date
1	Patrick Fisher, HR Advisor	New document	01/09/2023	01/09/2027