Privacy Notice for Staff

How we use your information – HR Privacy Notice for the University of Kent (Data Controller)

Version 1.4 – Updated August 2025

This privacy notice aims to communicate how we use your data in a concise manner in accordance with the UK GDPR Article 12, whilst meeting our statutory notice obligations (Articles 13 and 14). If you would like to know more then please contact our Data Protection Officer via the Data Protection web form or by emailing dataprotection@kent.ac.uk.

Contents

Data Protection Register

Our entry in the Information Commissioner's Office (ICO) Data Protection Register (Number Z6847902 [3]) contains details of types of information processed, who the information is about and who the information is shared with.

Definitions

Engagement - within this document, the term 'engagement' includes appointments under a contract of employment and/or other types of contract such as a worker contract or an external examiner or invigilator contract. It also includes Honorary or Visiting positions, Honorary Staff Associates, Contractors and/or sub-contractors plus other arrangements that require the creation of an IT account or HR/Payroll record.

Staff - Within this document, the term 'staff' includes individuals engaged under any of the arrangements described above.

Job - Within this document, the term 'job' includes any tasks, duties or activities carried out as part of the engagement arrangement.

How we collect your information

We collect many different types of personal data about you for lots of reasons. We cannot administer our employment or other relationship with you without your personal data. Where we don't need your personal data, we will make this clear, for instance we will explain if any data fields in our forms or staff survey processes are optional and can be left blank.

Further details of the personal data we collect, where we get it from and what we do with it are set out in **Schedule 1**.

You provide us with personal data directly when you apply for engagement with us, when you complete our application forms or correspond with us and in the course of performing your job. We also create some personal data ourselves and obtain some personal data from other sources. We obtain it from other people and organisations, including some public sources, such as publicly available directories and online resources, your emergency contacts, your use of University provided assets, systems and platforms, your line manager and co-workers, your dependants and beneficiaries and third party benefits providers.

If any of the personal information you have given to us changes, such as your contact details, please inform us without delay by updating your record in Staff Connect https://staffconnect.kent.ac.uk

Within this document, the term 'engagement' includes appointments under a contract of employment and/or other types of contract such as a worker contract or an external examiner or invigilator contract. It also includes honorary or visiting positions, honorary staff associates,

contractors and/or sub-contractors plus other arrangements that require the creation of an IT account or HR/Payroll record. Within this document, the term 'staff' includes individuals engaged under any of the arrangements described above.

The purposes of processing your information

We process your personal data for particular purposes in connection with your engagement with us, and the management and administration of our business.

We are required by law to always have a permitted reason or justification (called a "lawful basis") for processing your personal data. There are six such permitted lawful basis for processing personal data. The table at **Schedule 3** sets out the different purposes for which we process your personal data and the relevant lawful basis on which we rely for that processing.

Please note that where we have indicated in the table at **Schedule 3** that our processing of your personal data is either:

- necessary for us to comply with a legal obligation; or
- necessary for us to take steps, at your request, to potentially enter into an engagement with you, or to perform it

If you choose not to provide the relevant personal data to us, we may not be able to enter into or continue our engagement with you.

We may also convert your personal data into statistical or aggregated form to better protect your privacy, or so that you are not identified or identifiable from it. Anonymised data cannot be linked back to you. We may use it to conduct research and analysis, including to produce statistical research and reports. For example, to help us understand the diversity of the University's workforce and to make submissions to recognised diversity bodies such as Advance HE (for Athena Swan).

Once your engagement with us has ended, after a period of time your data will be removed from our HR systems and your basic details will be archived in a secure system visible to only a few members of HR. This will allow us to continue to provide engagement confirmation references for you and/or respond to other requests for basic engagement information.

Special Category Personal Data (including Criminal Offence Data)

We are required by law to treat certain categories of personal data with even more care than usual. These are called sensitive or special categories of personal data and different lawful bases apply to them.

The table at **Schedule 4** sets out the different purposes for which we process your special category personal data and the relevant lawful basis on which we rely for that processing. For some processing activities, we consider that more than one lawful basis may be relevant – depending on the circumstances.

Who your information is shared with

We ask third parties (e.g. service providers and/or sub-contractors) to carry out certain business functions for us, such as the administration of our payroll for staff based in Europe and the hosting of our HR IT systems (which will include maintenance, development and upgrade). These third parties will process your personal data on our behalf (as our processor). We will disclose your personal data to these parties so that they can perform those functions, however we will enter into a written contract imposing appropriate security standards on them to ensure that they have appropriate security standards in place to protect your personal data. The table at **Schedule 5** provides further details of the key service providers who process staff personal data on our behalf ('data processors').

Your personal data may also be shared between colleagues who legitimately need the information to carry out their duties, for example SAT teams for Athena Swan submissions. Your personal data may also be shared, in limited circumstances, with your Trade Union or nominated representative.

Registration with IT means that a member of staff's name, department/section, email address and telephone number will appear in the University's internal email and telephone directory. This information may also appear on externally facing departmental webpages.

Registration for an IT account means that an individual's name, department/section, email address and telephone number will appear in the University's internal email and telephone directory. This information may also appear on externally facing departmental webpages.

Staff photographs are used on security cards for the purposes of identification and security.

The University may occasionally commission photographs around Campus or at specific University events which could include images of staff for inclusion in promotional material.

We may also share your information with other departments in the University for the purposes of administering your engagement benefits (including salary sacrifice arrangements).

The University may monitor IT use through user names and log-ins to ensure adherence to the Acceptable Use Policy, and for legal, security or for statistical purposes. Device location data is also monitored by our device-as-a-service provider, Apogee. We also use automated processing (including AI) for monitoring purposes, for example, Microsoft Defender for Endpoint to protect the security of our IT infrastructure. Please see **Schedule 5** for further details.

In certain circumstances, we will also disclose your personal data to third parties who will receive it as controllers of your personal data in their own right for the purposes set out above, in particular:

- if we transfer, purchase, reorganise, merge or sell any part of our organisation or the organisation of a third party, and we disclose or transfer your personal data to the prospective seller, buyer or other third party involved in a transfer of undertaking, reorganisation or merger arrangement (and their advisors); and
- if we need to disclose your personal data in order to comply with a legal obligation, to enforce a contract or to protect the rights, property or safety of our staff, collaborative partners, students or others.

We have set out below a list of the categories of recipients with whom we are likely to share your personal data:

- staff-related benefits providers and other third parties in connection with your benefits (such as pension trustees);
- clients;
- consultants and professional advisors including legal advisors and accountants;
- courts, court-appointed persons/entities, receivers and liquidators;
- partners and joint ventures;
- trade associations and professional bodies;
- security partners including, for example, operators of the University car parks;
- insurers; and
- governmental departments, statutory and regulatory bodies including the

Department for Work and Pensions, Information Commissioner's Office, the police, Her Majesty's Revenue and Customs, the Office for Students and the Higher Education Statistics Agency.

Further details of the data controllers who we share staff data with are available in **Schedule 6**.

We may also share your personal data with third parties, as directed by you.

Finally, the University operates a number of electronic HR systems within which the personal data referred to in **Schedule 1** is stored. Managers have access to the personal data of staff in their management hierarchy in order to effectively and efficiently conduct appropriate management of those members of staff. Managers are only granted access to this information on the basis that:

- they are trusted to access the data only at a time, and to the extent, necessary to conduct appropriate management of the relevant staff member;
- they access it in accordance with this privacy notice, the University's Data Protection policy and the University's obligations under GDPR;
- they have undertaken appropriate and relevant data protection training; and
- they access the information in accordance with the University's IT Regulations.

Any inappropriate accessing of personal data could be regarded as gross misconduct.

Where in the world is your personal data transferred to?

If any of our processing activities require your personal data to be transferred outside the United Kingdom we will only make that transfer if:

- the country to which the personal data is to be transferred ensures an adequate level of protection for personal data as determined by the Secretary of State:
  Department for Science, Innovation and Technology UK adequacy
  What countries or territories are covered by adequacy regulations? (ICO website)

- we have put in place appropriate safeguards prescribed by the UK GDPR (or EU GDPR if applicable) to protect your personal data, such as an appropriate contract with the recipient containing the EU Standard Contractual Clauses and the UK ICO Addendum or the ICO's International Data Transfer Agreement (IDTA). Further information here: *Is the*

restricted transfer covered by appropriate safeguards? (ICO website)

- the transfer is necessary for one of the reasons specified in data protection legislation, such as the performance of a contract between us and you; or

- you explicitly consent to the transfer.

How long do we keep your personal data for?

If you are engaged by us we will keep your personal data during the period of your engagement and then, after your engagement with us ends, for as long as is necessary in connection with both our and your legal rights and obligations. This may mean that we keep some types of personal data for longer than others. Full details of our data retention periods are contained in **Schedule 2**.

We will only retain your personal data for a limited period of time. This will depend on a number of factors, including:

- any laws or regulations that we are required to follow;
- whether we are in a legal or other type of dispute with each other or any third party;
- the type of information that we hold about you; and
- whether we are asked by you or a regulatory authority to keep your personal data for a valid reason.

Any personal data contained in any work related correspondence or records may be retained for longer, dependent on the retention period of the file that your personal data is held on.

Automated decision-making, profiling and AI use

You have the right to be informed about the existence of any automated decision-making (which would include the use of Artificial Intelligence (AI) and include any profiling of you) in cases where the decision significantly affects you or produces legal effects concerning you. We will provide you with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you. Unless the decision making is necessary for a contract with you, based on your explicit consent or required by law you have the right not to be subject to a decision based solely on automated processing. Where a decision is based on a contract with you or your consent we will implement measures to safeguard your rights and at least the right to obtain human review of the decision.

We currently use automated processing and AI for network and device security monitoring purposes. Any activity which results in restriction of a device will involve human intervention to review the security alert automatically generated.

Where our software applications use or are AI enabled these are marked with a * in Schedules 5 and 6 below.

Generative AI use

We currently have the use of Microsoft's Copilot Chat available within our Microsoft 365 tenancy for education and accessed using a Kent IT account. This enables staff and students to get answers to questions via prompts using a chat based interface. Although staff are instructed not to put personal or sensitive data into Copilot Chat we recognise AI may process personal data in the course of generating responses. We rely on public task as our lawful basis for our core teaching and learning purposes and legitimate interests and (where applicable) legal obligation for incidental processing (e.g. monitoring). Any retained outputs generated by Copilot Chat (or any other permitted generative AI tool) will be reviewed and verified for accuracy. **Staff should be aware that outputs of generative AI systems are statistically informed guesses/inventions rather than facts**.

Microsoft's privacy and security information for Copilot Chat can be viewed here: https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-transparency-note?view=o365-worldwide

Microsoft's privacy notice (relevant to Bing enabled searching) is here: https://www.microsoft.com/en-gb/privacy/privacystatement

We will review our AI and generative AI use and practices to ensure these and any emerging risks are monitored. Limited authorised staff may check audit logs for security monitoring purposes or generate reports which indicate active users (name and email address or IP address and device location). In the event an information request or complaint is received audit log data (such as time and date of queries and if Bing was used), or prompt and response data may be reviewed. Prompts and responses can be deleted directly by users, although : https://support.microsoft.com/en-gb/office/delete-your-microsoft-365-copilot-activity-history-76de8afa-5eaf-43b0-bda8-0076d6e0390f

For more detailed information regarding the use of Generative Artificial Information at the University of Kent, please click here.

Your rights

You have certain legal rights, which are briefly summarised below, in relation to any personal data about you which we hold. These can be accessed free of charge by contacting dataprotection@kent.ac.uk:

Your right	What does it mean?	Limitations and conditions of your right
Right of access	Subject to certain conditions, you are entitled to have access to your personal data (this is more commonly known as submitting a "data subject access request").	If possible, you should specify the type of information you would like to see to ensure that our disclosure is meeting your expectations. We must be able to verify your identity. Your request may not impact the rights and freedoms of other people, e.g. privacy and confidentiality rights of other staff.
Right to data portability	Subject to certain conditions, (**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/**) you are entitled to receive the personal data which you have provided to us and which is processed by us by automated means, in a structured, commonly-used machine readable format.	If you exercise this right, you should specify the type of information you would like to receive (and where we should send it) where possible to ensure that our disclosure is meeting your expectations. This right only applies if the processing is based on your consent or on our contract with you and when the processing is carried out by automated means (i.e. not for paper records). It covers only the personal data that has been provided to us by you.

Rights in relation to inaccurate personal or incomplete data	You may challenge the accuracy or completeness of your personal data and have it corrected or completed, as applicable. You have a responsibility to help us to keep your personal information accurate and up to date. We encourage you to notify us of any changes regarding your personal data as soon as they occur, including changes to your contact details, telephone number or immigration status.	Please always check first whether there are any available self-help tools to correct the personal data we process about you. This right only applies to your own personal data. When exercising this right, please be as specific as possible.
Right to object to or restrict our data processing	Subject to certain conditions, you have the right to object to or ask us to restrict the processing of your personal data.	As stated above, this right applies where our processing of your personal data is necessary for our legitimate interests. You can also object to our processing of your personal data for direct marketing purposes.
Right to erasure	Subject to certain conditions, you are entitled to have your personal data erased (also known as the "right to be forgotten"), e.g. where your personal data is no longer needed for the purposes it was collected for, or where the relevant processing is unlawful.	We may not be in a position to erase your personal data, if for example, we need it to (i) comply with a legal obligation, or (ii) exercise or defend legal claims.
Right to withdrawal of consent	As stated above, where our processing of your personal data is based on your consent you have the right to withdraw your consent at any time.	If you withdraw your consent, this will only take effect for future processing.

Your rights: withdrawal of consent

Where our processing of your personal data is based on your **consent**, you have the right to withdraw your consent at any time. If you do decide to withdraw your consent we will stop processing your personal data for that purpose, unless there is another lawful basis we can rely on – in which case, we will let you know. Your withdrawal of your consent won't impact

any of our processing up to that point.

Your rights: legitimate interests

Where our processing of your personal data is necessary for our **legitimate interests**, you can object to this processing at any time. If you do this, we will need to show either a compelling reason why our processing should continue, which overrides your interests, rights and freedoms or that the processing is necessary for us to establish, exercise or defend a legal claim.

Your right to lodge a complaint to the Information Commissioner

You also have the right to lodge a complaint with the Information Commissioner's Office, which is the UK data protection regulator. More information can be found on the Information Commissioner's Office website at https://ico.org.uk/.

For further guidance regarding your rights please see the ICO website: https://ico.org.uk

You will not have to pay a fee to exercise your rights. However if your request is unfounded or excessive, we may charge a reasonable fee in line with our Schedule of charges for information requests as detailed on our freedom of information requests page, or alternatively, refuse to comply with the request.

Please consult our data protection rights page of our website and Data Subject Rights Policy for further information and contact data protection if you would like to make a request.

Further processing of your data

Where required, we will provide further privacy notices to you to ensure that we are transparent, accountable and you have control in how we use your personal information.

Your obligations

The University tries to ensure that the information it holds is accurate and up-to-date. It must, however, rely on individuals to inform the appropriate office of any change in their personal data. In particular, any change of home address or emergency contact details. This can be done directly in Staff Connect.

As a user you are required to comply with the University's IT regulations for the use of

computing facilities. It is also your responsibility, should you hold personal data on others, to ensure that you abide by the terms of Data Protection law.

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:

https://www.kent.ac.uk/about/assurance-and-data-protection/data-protection-rights-and-subject-access-requests

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

Or by writing to: The Data Protection Officer, The University of Kent, The Registry, Canterbury, Kent CT2 7NZ.

SCHEDULE 1 – Categories of Personal Data

Type of personal data
a) Contact information
• Name(s) • Known as names(s) • Address(es) • Email address(es) • Contact details including mobile telephone number(s)
b) **Personal Information**
• Date of birth • Gender Identity / Sex • Next of kin or other dependants • Marital or relationship status • Lifestyle and social circumstances • Emergency contact information
c) **Identity and Background Information**
• Details of education and qualifications and results • Career history, experience and skills • Passport information • Driving licence information • Psychometric test results • Right to work, residency and/or other visa information (where unrelated to your race or ethnicity) • Curriculum Vitae (CV) or resume and professional profile • Image or photographs • Application form • Evaluative notes and decisions from job interviews • Preferences relating to job location and salary • Conflicts of interests (including where related to family networks)

d) **Financial Information**

- Bank account details
- Salary, compensation and other remuneration information
- National insurance number and/or other governmental identification numbers
- Business expense and reimbursement details

e) **Special Category or Criminal Offence Personal Data**

- Racial or ethnic origin (including your nationality and visa information)
- Religious or philosophical beliefs
- Trade union membership
- Data concerning physical and/or mental health (including occupational health requirements, accident reports, day-to-day health concerns such as diabetes or epilepsy conditions which we should be aware of, dietary requirements, allergies and reasons for any short term or long term absence)
- Sexual orientation
- Health and safety and accident records and reports
- Information relating to actual or suspected criminal convictions and offences
- Biometric data (where you have opted to use Windows Hello for device user authentication purposes)

f) **Engagement Administration Information**

- Terms and conditions of engagement
- Work related contact details (including location and office and corporate phone numbers)
- Image/photographs
- Holiday and other leave related records
- Your working preferences and feedback in relation to the University and our staff
- Your preferences in relation to our use of your personal data
- Hours worked and working time preferences
- Statutory and non-statutory leave and absence records
- Job termination details

g) **Job Performance Information**

- Role responsibilities
- Personal development reviews and appraisals, and associated feedback
- Training records
- Attendance information, including clocking in/out systems or timesheets
- Promotion and salary award applications and/or outcome records
- Transfer and secondment information
- Academic and research publications

h) **Investigation, Grievance and Disciplinary**

- University investigations records
- Grievance and disciplinary records
- Employment tribunal records

i) **Benefits Information**

- Pensions memberships for you and/or your dependants or other beneficiaries
- Salary sacrifice scheme membership,
- Childcare vouchers purchase
- Cycle to Work scheme membership

j) **Systems Usage**

- Access logs and usage records from HR and other IT systems
- Diagnostic, telemetry and other device data
- User IDs
- IP addresses
- Telephone systems use logging and voicemail

k) **Security, Location and Access Information**

- Images or access data captured or recorded by electronic card access systems, CCTV and other security control systems
- Information (including image, location and time stamp) captured or recorded by the Kent Player lecture capture system
- Information on staff space allocation and location captured by facilities management software
- device location tracking and timestamp data for device management and attendance monitoring purposes
- journey data when you use our campus shuttle service
- Telephone call recordings (security and emergency numbers)

SCHEDULE 2 – HR Data Retention Schedule

Record type	Suggested retention period	Exceptions
Recruitment documentation: employment/engagement application forms (including budget & authorisation documents). To also include: Advert, screen shots, shortlisting grid, interview notes for all unsuccessful resident shortlisted candidates, shortlisted applications, number and names of shortlisted candidates	For unsuccessful applicants: the data will be anonymised 1 year after the successful candidate commences engagement For successful candidates, 7 years following end of engagement	If the successful candidate requires sponsorship then the retention period (in respect of application forms, CVs and other documents) will be in line with UKVI requirements. UKVI requirement: Documents must be kept for whichever is the shorter period: • One year from the date sponsorships ends • The point at which a compliance officer has examined and approved them.
References received during engagement process User accounts created by applicants during the hiring process	For unsuccessful applicants: the data will be anonymised 1 year after the successful candidate commences engagement For successful candidates: 7 years following end of engagement	Where a staff member requires sponsorship but no resident labour market test was undertaken (Tier 4 switch for example), references must be held in line with UKVI requirements.

	Accounts will be deleted following 14 months of inactivity	
Relocation expense claims and supporting documents	7 years following end of engagement	
DBS checks	Data required to undertake the check and the results of the check will be retained according to the GBG Data Retention Schedule A note that the check results were satisfactory will be retained until 7 years following end of engagement	Where a staff member requires sponsorship, and a DBS check is a requirement of the role, then the DBS check will be retained in line with UKVI requirements as above
Right to work checks	7 years following end of engagement	
Equal opportunities monitoring data provided during the hiring process:	Recruitment System: For unsuccessful applicants: the data will be anonymised 1 year after the successful candidate commences engagement For successful candidates: 7 years following end of engagement	Data may also be anonymised and stored in statistical form indefinitely
EDI data provided during engagement	7 years following end of engagement	Data may also be anonymised and stored in statistical form indefinitely

Written particulars of engagement, contracts of engagement and changes to terms and conditions	7 years following end of engagement	
Job description:	Recruitment System: For unsuccessful applicants: the data will be anonymised 1 year after the successful candidate commences engagement For successful candidates, 7 years following end of engagement	
Documents authorising changes to contract e.g. budget/finance information (DB501)	7 years following end of engagement	
Working time opt-out forms and records to show compliance with Working Time Regulations	7 years following end of engagement	
Leave Records	7 years following end of engagement	
Sickness records	7 years following end of engagement	
Appraisal / assessment or training records (e.g. RPD, Probation, REF, training assessment)	7 years following end of engagement	
Details of qualifications, mandatory training /skills	7 years following end of engagement	
Records relating to promotion/salary award	7 years from end of engagement	

Study Leave applications	7 years following end of engagement	
Records relating to disciplinary or grievance matters, or Dignity at Work complaints	7 years following end of engagement	May include images / voice recordings / time & location data captured or recorded by electronic card access systems, CCTV and other security control systems.
References given or information needed to provide a reference	7 years following end of engagement	Where a staff member requires sponsorship but no resident labour market test was undertaken (Tier 4 switch for example), references must be held in line with UKVI requirements.
Records relating to accidents or injury at work	7 years following end of engagement	
Records relating to Occupational Health reports	7 years following end of engagement	
Data protection consent forms	7 years following end of engagement	
Email correspondence to/about the individual held within HR	7 years following end of engagement	Or, if relevant to the subject matters contained elsewhere in this Schedule, in accordance with the specific retention periods as set out
IT access requests	7 years following end of engagement	

Records relating to a Visiting or Honorary appointment	7 years following end of engagement	
Settlement agreements and associated documents	7 years from end of engagement	
Documents associated with termination of engagement (retirement, redundancy dismissal, resignation etc.)	7 years from end of engagement	
Archived data following deletion 7 years from end of engagement. To include: basic engagement details such as name, job title, pay grade, engagement start and end dates.	15 years from end of engagement	
Copilot chat audit log data, Copilot prompts and responses	1 year 2 years (or until IT account is deleted)	Where these are requested as part of a subject access request, litigation hold or disciplinary matter (see category above).
IT telemetry, device and audit logs and feedback Biometric authentication	Up to 2 years Until consent is withdrawn or device reassigned	Unless held for longer where related to one of the categories above (e.g. legal obligation/litigation hold).
Telephone calls to campus security	Stored for 28 days	Unless marked for longer for a specific reason (e.g. legal obligation/litigation hold)

All employee data in the above categories held in other areas of the University	In accordance with the specific retention periods as set out in this schedule	Or in accordance with the holding area's published Data Retention Schedule if this is a longer period or where the purpose is archiving in the public interest.

SCHEDULE 3 – Purposes of Processing Personal Data

For some processing activities, we consider that more than one lawful basis may be relevant - depending on the circumstances.

Purposes of processing	**Lawful basis** We are permitted to process your personal data because…					
	1. You have given **your consent** to the processing	2. It is necessary to perform your engagement contract	3. It is necessary for us to comply with a legal obligation	4. It is necessary for our legitimate interests or those of third parties	5. It is necessary to protect your vital interests (or those of someone else)	6. It is necessary to perform a task in the public interest or in our official authority
a) **Recruitment and workforce planning**						

1. Administering your application for a job with us and considering your suitability for the relevant role				✓		
2. Obtaining, considering and verifying your engagement references and employment history				✓		
3. Reviewing and confirming your right to work in the UK			✓			

4. Conducting verification and vetting, including criminal background checks and credit checks where required by law			✓			
5. Conducting background checks, verification and vetting which are not required by law but needed by us to assess your suitability for your role	✓					✓
6. Making a job offer to you and entering into a contract of engagement with you		✓				

7. Identifying and assessing the University's strategic business direction and resourcing needs, current staff and areas for development				✓		
8. Promotion and succession planning				✓		
9. Analysing recruitment and retention objectives, processes and staff turnover rates				✓		
10. Developing, operating and collecting feedback on recruitment activities and staff selection processes				✓		

b) **General engagement management and administration**						
11. Communicating with you and providing you with information in connection with your engagement with us from time to time		✓		✓	✓	
12. Paying your salary, compensation and any other benefits pursuant to your contract of engagement		✓				
13. Calculating and administering taxation within payroll, and your entitlements to any statutory/contractual benefits (including statutory sick pay and workforce pension arrangements)			✓			

14. Facilitating the administration of any private healthcare, life assurance/insurance, pensions initiatives and plans that we offer in connection with your engagement with us			✓	✓		
15. General staff administration, including workforce management and facilities operations				✓		
16. Managing our health and safety compliance obligations			✓			

17. Paying you discretionary or non-contractual benefits or managing and administering salary sacrifice arrangements (including, for example, nursery vouchers and discounted gym membership)	✓			✓		
18. Managing annual leave entitlement and records, and to administer related payments				✓		
19. Managing absence records, contractual sick leave entitlement and administering related payments		✓		✓		

20. Managing maternity, paternity, adoption, parental and dependants leave and (where applicable) pay			✓			
21. Contacting the appropriate person in the event of an emergency concerning you					✓	
22. Administering our insurance policies				✓		
23. Determining whether any adjustments are necessary to enable you to carry out your role		✓	✓			
24. Preparing risk assessments to prevent future injuries in the workplace			✓			

25. Carrying out performance reviews				✓		
26. Allocating and assigning responsibilities as necessary for workload management purposes, and measuring staff utilisation				✓		
27. Administering, recording and analysing training and training records				✓		
28. Supporting the establishment and maintenance of staff directories				✓		
29. Considering your continuous suitability for your role				✓		

30. Providing details of your engagement to a new or potential employer, bank or financial institution where requested by you	✓					
31. Handling grievance and disciplinary matters, including investigating issues, considering appropriate resolution and mitigating actions and reviewing outcomes				✓		
32. Responding to reference requests from your future potential employers				✓		
c) **Security and governance**						

33. Monitoring the security of the University's physical premises (including car parks) and systems, networks and applications			✓	✓		
34. Identifying and authenticating staff and other individuals	✓			✓		
35. Establishing a network of emergency contacts for individuals in case of emergency				✓		
36. Identifying, investigating and mitigating suspected misuse of the University's assets, systems and platforms			✓	✓		✓

37. Ensuring compliance with the University's policies and procedures				✓		
d) **Legal and regulatory compliance and responsibilities**						
38. Managing and administering our equal opportunities reporting			✓			
39. Compliance with obligations under the contract of engagement between you and the University		✓				
40. Responding to binding requests or search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities			✓			✓

41. Responding to non-binding requests or search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities				✓		
42. Complying with disclosure orders arising in civil proceedings			✓			✓

43. Investigating, evaluating, demonstrating, monitoring, improving, reporting on and meeting the University's compliance with relevant legal and regulatory requirements			✓			✓
44. Investigating, evaluating, demonstrating, monitoring, improving, reporting on and meeting the University's compliance with best practice and good governance responsibilities				✓		

45. Responding to employment and industrial relations matters where permitted by applicable law, including criminal investigations, grievances, arbitrations, negotiations, elections and strikes			✓	✓		✓
46. Responding to binding requests from collaborative and commercial partners of the University.			✓			
47. Responding to non-binding requests from collaborative and commercial partners of the University.				✓		

48. Preparing and submitting applications to commercial and collaborative partners, Government agencies and non-departmental public bodies.				✓		
e) **Day-to-day business operations**						
49. Implementing, adapting and enhancing systems and processes to develop or improve our business and/or make your job easier or more enjoyable				✓		
50. Managing, planning and delivering our global business, sales and marketing strategies				✓		

51. Supporting our diversity programmes and staff support networks and initiatives	✓			✓		
52. Publishing external facing materials for marketing and public relations purposes such as where we mention you in the context of the University's projects and initiatives in our marketing materials, social media posts and press releases				✓		
53. Administering your travel and accommodation arrangements		✓	✓	✓		

54. Supporting and maintaining our technology infrastructure		✓		✓		
55. Supporting the sale, transfer or merging of part or all of our business or assets, or in connection with the acquisition of another business			✓	✓		

SCHEDULE 4 – Purposes of Processing Special Category Data

Purposes of processing	**Special category lawful basis** We are permitted to process your personal data because…						
	1. You have given **your explicit consent** to the processing	2. It is necessary for your/our obligations and rights in the field of **employment and social security** and social protection law	3. It is necessary to protect the **vital interests** of the data subject or another person you or they are physically or legally incapable of giving consent	4. It is necessary for our establishment, exercise or defence of **legal claims**	5. It is necessary for reasons of **substantial public interest**	6. It is necessary for **preventive or occupational medicine**, for the assessment of the working capacity of the employee	7. The processing relates to personal data which are manifestly made public by the data subject
a) **Recruitment and workforce planning**							
1. Conducting verification and vetting, including criminal background checks and		✓			✓		

credit checks where required by law							
2. Conducting background checks, verification and vetting which are not required by law but needed by us to assess your suitability for your role	✓				✓		
b) **General engagement management and administration**							
3. Facilitating the administration of any trade union subscriptions, private healthcare, life assurance/insurance, pensions initiatives and plans that we offer in connection with your engagement with us	✓	✓			✓		

4. Managing absence records, contractual sick leave entitlement and administering related payments		✓			✓		
5. Contacting the appropriate person in the event of an emergency concerning you			✓				
6. Administering our insurance policies					✓		
7. Determining whether any adjustments are necessary to enable you to carry out your role		✓					
c) **Security and governance**							
8. Identifying and authenticating employees and other individuals	✓				✓		

9. Identifying, investigating and mitigating suspected misuse of the University's assets, systems and platforms				✓			
d) **Legal and regulatory compliance and responsibilities**							
10. Managing and administering our equal opportunities reporting					✓		
11. Responding to binding requests or search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities or sharing information (on a voluntary basis) with the same				✓			

12. Complying with disclosure orders arising in civil proceedings				✓			
13. Investigating, evaluating, demonstrating, monitoring, improving and reporting on the University's compliance with relevant legal and regulatory requirements				✓			
14. Responding to and investigating engagement and industrial relations matters where permitted by applicable law, including criminal investigations, grievances, arbitrations, negotiations, elections and strikes		✓		✓			

15. Making reasonable adjustments as needed to help remove barriers faced by you in your role because of any disability you might have		✓					
16. Delivering occupational health advice and services to you in relation to your role with us						✓	
17. Responding to binding requests from collaborative and commercial partners of the University.	✓				✓		
18. Responding to non-binding requests from collaborative and commercial partners of the University.	✓				✓		
19. Preparing and submitting applications to commercial and collaborative partners, Government agencies and	✓				✓		

non-departmental public bodies.							
Ascertaining and investigating any suspected breaches (by staff or the University) of legal rights or obligations granted or imposed by employment law, including where necessary the use of CCTV footage.		✓	✓	✓			
e) **Day-to-day business operations**							
20. Supporting our diversity programmes and staff support networks and initiatives	✓				✓		
22. Administering facility time and publicising contact details for trade union representatives	✓				✓		

SCHEDULE 5 – Data Processors

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 terms are included to ensure compliance with data protection laws and that the data is used solely under our instruction. In these circumstances personal data will be deleted or returned to us after the contract has terminated. Where you complain about a third party provider who is providing services on behalf of the University your complaint will be shared with them (although we will obtain your permission before sharing confidential health information).

Some of our key service providers are listed below:

Provider	Purpose	Location	Lawful Transfer basis
Microsoft (MS Office 365, MS Forms)	IT infrastructure Microsoft privacy notice	United States (with data hosted in the EU). If necessary they transfer the data to their sub-processors (see their sub-processor list here)	Microsoft's data processing contract incorporating the EU Standard Contractual Clauses and ICO Addendum can be viewed here. Further details about the safeguards it puts in place are here.
Tribal Group PLC (Kent Vision)	Student Data Management System Tribal Privacy Notice	United Kingdom	N/A
Moodle Pty Ltd	Virtual learning environment and training delivery Moodle privacy notice	Australia	The EU Standard Contractual Clauses and ICO Addendum can be viewed here
Stonefish Software Ltd	e-Recruitment system	United Kingdom	N/A

Zellis UK Ltd (Staff Connect)	Employee management system Zellis privacy notice	HQ is in the United Kingdom	N/A (processor relies on ICO Addendum for sub-processor transfers).

Other Key Providers A-Z	**Purpose**	**Location**	**Lawful Transfer basis**
Adobe Systems Software Ireland Limited (Adobe Ireland)*	Various applications for business and teaching purposes (graphics, visualisation and multi media). Adobe privacy notice	EEA with data stored in United States	Adequacy decision (see Adobe Privacy Centre for more details)
Apogee Corporation Ltd	Online print and device and IT asset management DaaS provider. Apogee privacy notice.	United Kingdom, Ireland and Germany	Adequacy decision
Auga Technologies Ltd and Auga Technologies Inc (Vevox)*	Live polling app Vevox privacy notice	United States with data stored in Ireland (managed by Amazon Web Services)	Adequacy decision
Britannic Technologies Ltd	Telephony Services	United Kingdom	N/A
Civica Occupational Health See our OH privacy notice	OH record management system Civica privacy notice	United Kingdom (data storage); Germany (scheduling) and the United States (messaging)	N/A
Cultureshift Communications Ltd ('Culture Shift')	Report & Support online reporting system Cultureshift Privacy Notice	United Kingdom	N/A
Communis Ltd (trading as ISARR)	Health and Safety and security incident reporting software.	United Kingdom	N/A

	https://isarr.com/privacy-policy/		
Digital Interactive Ltd (who provide Infreemation)	Case management system for statutory FOI and UK GDPR requests Digital Interactive privacy notice	United Kingdom	N/A
Diligent Corporation	For minuting and management of governance and committee meetings (if you attend as a staff member) Diligent privacy notice	United States	UK Extension to the EU-US Data Privacy Framework
Diversity Travel Ltd	Travel management and booking	United Kingdom	N/A
Docusign International (EMEA) Limited	Electronic signature tool	Ireland (although data residency is UK based personal data may be transferred within the Docusign Group including Docusign, Inc in the United States and to other sub-processors).	Adequacy (with intergroup or sub-processor transfers governed by Binding Corporate Rules Standard Contractual Clauses (and UK/ICO Addendum)
EPOS Now (UK) Ltd	Payment processing Epos Now privacy notice	United Kingdom	N/A
Flywire Inc (formerly WPM Education Ltd)	Payment processing. Flywire privacy notice	United States	UK Extension to the EU-US Data Privacy Framework
Imperial Civil Enforcement Solutions Ltd or iCES 360 and Permitsmarti	Parking enforcement and issuing permits ICES privacy notice	United Kingdom	N/A

Invida Ltd	Facilities Management and Staff space allocation management system Invida privacy notice	United Kingdom	N/A
Jamworks *AI Note taker (via Jisc)	AI enabled notes and flashcards enabled from Panopto lectures. Jamworks privacy notice	United Kingdom AWS London instance	N/A
Jisc's 'Online Surveys' (for Advance HE)	Surveys for national research purposes (de-identified data) JISC online surveys privacy notice Advance HE privacy notice	United Kingdom	N/A
Jotform, Ltd (part of Jotform Inc)	Form filling functionality Jotform privacy notice	United States	UK addendum to the EU SCCs UK extension to the EU-US Data Privacy Framework
Key Travel Ltd	Travel management and booking	European Economic Area	Adequacy decision
Kinetic Solutions Ltd	Conference, catering and student accommodation management system Kinetic Software privacy notice	United Kingdom	N/A
Monday Inc	Project and task tracking Monday.com privacy notice	United States (Stored by Amazon Web Services)	UK Extension to the EU-US Data Privacy Framework
One Advanced Central Management Information System (CMIS and CMISGo)	Timetabling software Online room booking system One Advanced Privacy Policy	United Kingom, EU, USA, Canada, India and Australia	One Advanced Privacy Policy

Panopto Inc	For recording lectures Panopto privacy notice	United States	UK Extension to the EU-US Data Privacy Framework Panopto privacy notice
Pop Inc (Wordfly)	Delivery of event information Wordfly privacy notice	United States	UK Extension to the EU-US Data Privacy Framework Standard Contractual Clauses
Qlik (for Qliksense* and Qlikview)	Business intelligence tools for planning purposes Qlik privacy notice	United States and United Kingdom Qlik subprocessors list	UK Extension to the EU-US Data Privacy Framework Qlik privacy notice
Qualtrics*	Surveys Qualtrics data protection and privacy page	United States and worldwide subprocessor list	Standard Contractual Clauses Qualtrics data protection and privacy page
Sagoss Ltd	ANPR parking management system Sagoss privacy notice	United Kingdom	N/A
Simac IDS BV (Presto)	Student engagement and attendance monitoring ('SEAM') system Simac privacy notice	The Netherlands	Adequacy decision Simac privacy notice
Technology One UK Ltd (Course Loop)	Curriculum Management System Course loop privacy notice	United Kingdom (storage) Sub-processor locations	Standard Contractual Clauses
Tessitura Network Inc	Gulbenkian box office system Tessitura privacy notice	United States	Tessitura privacy notice
TOPdesk UK Ltd	IT support management system TOPdesk privacy notice	United Kingdom	N/A
Unit 4 Group Holding BV Unit 4 Enterprise Resource Planning (formerly Agresso Business World)	Our central finance accounting system Unit 4 privacy notice	The Netherlands	Adequacy decision Unit 4 privacy notice

Western Union Payment Services GB Ltd (subsid of Western Union Holdings Inc)	Overseas payment processing Western union privacy notice	United Kingdom and United States	Standard Contractual Clauses Western union privacy notice
Worktribe Ltd	Research grant support case management system Worktribe privacy notice	United Kingdom	N/A
XN Leisure Systems Ltd (part of Jonas companies)	Sports centre membership management XN leisure privacy notice	United Kingdom and United States	Standard Contractual Clauses XN leisure privacy notice
Zeelo Ltd (where you have opted to use the service)	Campus Shuttle bus provider Zeelo privacy notice	Data is hosted in a United Kingdom data centre but may be processed elsewhere by subprocessors including the EEA and United States	Standard Contractual Clauses Zeelo privacy notice

*AI enabled

SCHEDULE 6 –Third Party Data Controllers

We share your personal data with third party **data controller(s)** where we are required by law to do so or where those third party organisations have a legitimate reason to use your data for their own purposes. Our data protection policy requires that we ensure a Data Sharing Agreement is put in place to protect the use of your personal data. We will ensure that only the minimum information necessary to fulfil the purpose is shared.

We are a signatory to the Kent and Medway Information Sharing Agreement and where possible we will use that data sharing agreement for sharing with other signatories. For more information please see the Kent and Medway Information Partnership.

The organisations and circumstances where we most commonly share your personal data are listed below:

Partner	Purpose	Privacy Notice
Benenden	Corporate health membership scheme (where you apply)	Benenden privacy notice
Care First Ltd	Counselling Service	Care First privacy notice
Edenred/Reward Gateway (UK) Ltd Unum Dental	Reward platform offering discounts to staff including dental cover via Edenred.	Edenred privacy notice Reward Gateway privacy notice Unum Dental privacy notice
Pluxee UK Ltd	Employee Assistance Programme administrators	Pluxee privacy notice
Salary Finance Ltd	Loans repayable by salary deduction	Salary Finance privacy notice
UKAT (UK Advising and Tutoring)	Providing academic advisor training	UKAT privacy notice
Canterbury Christ Church University	Kent and Medway Medical School (KMMS)	KMMS privacy notice
Greenwich University	Medway School of Pharmacy staff data for their HESA return	

Our educational partner providers: Oxford International Education Group (OIEG) and Kent International College Limited	For the purposes of our embedded international college.	OIEG privacy notice UKIC privacy notice
Partner universities or HEIs	Where we collaborate for specific projects e.g. research projects	As applicable.
Higher Educational Statistical Agency (HESA) (now merged with the Joint Information Systems Committee (JISC))	We are required by law to share monitoring data and the data of new graduates.	HESA privacy notice
Office for Students (OfS)	Higher Education regulator in England.	OfS privacy notice
The Home Office in connection with UK Visas and Immigration Office	For immigration law purposes and to meet our obligations as a visa sponsor.	UK VI and Home Office privacy notice
UK Research and Innovation (UKRI) or other grant funding organisations	When processing grant, research and scholarship applications and payments.	UKRI privacy notice
Kent Students' Union	Administration of KSU matters such as: elections and democratic purposes; of KSU membership and activities; compliance with the University's non-academic misconduct regulations.	Kent Union privacy notice
Greenwich Student Union	For Medway students where necessary as part of our processes (for example where they are supporting you with a complaint).	Greenwich SU privacy notice
Education and Skills Funding Agency (ESFA)	Administers funding to deliver education and skills (NB moving into the Department of Education from March 2025).	ESFA privacy notice
Office for the Independent Adjudicator for Higher Education (OIA)	Body appointed under the Higher Education Act 2004 to run the student complaint scheme.	OIA privacy notice
Office for Standards in Education, Children's	Non-ministerial government department	Ofsted privacy notice

Services & Skills (Ofsted)	which inspects and regulates services for children and young people.	
Charity Commission	Independent regulator of Charities for England and Wales.	Charity Commission privacy notice
The British Council	The UK's international organisation for cultural relations and educational opportunities.	British Council privacy notice
His Majesty's Revenue and Customs (HMRC)	For tax and gift aid purposes.	HMRC privacy notice
Higher Education Access Tracker (HEAT)	Kent is the lead organisation for this collaboration of members tracking academic progression of pupils and students for wider participation in higher education purposes.	https://heat.ac.uk/privacy-notice/
Information Commissioner's Office	For regulatory reporting of data breaches or privacy complaints.	ICO privacy notice
Office for Sanctions Implementation (OFSI) or other related central government department (such as Export Control Joint Unit etc)	For regulatory licensing or reporting.	OFSI privacy notice
External bodies offering services (e.g. counselling services, Pluxee, Carefirst)	For confidential advice (where you have agreed and provided us with your permission).	See relevant organisation's privacy notice.
The Disclosure and Barring Service (DBS)	For checking suitability for some roles working with children or vulnerable people.	DBS privacy notices
Bodies responsible for professional accreditation	To confirm the accreditation and validity.	See relevant organisation's privacy notice.
Potential employers or education providers	Where you have asked us to provide a reference.	See relevant organisation's privacy notice.
Professional bodies such as the NHS or other	To confirm your qualifications.	See relevant organisation's privacy notice.

employers		NHS England privacy notice
Event venue providers	Where necessary for accessibility and assistance requirements.	See relevant organisation's privacy notice.
Drivers and Vehicles Licensing Agency (DVLA)	For parking enforcement.	DVLA privacy policy
Our auditors	For audit and best practice benchmarking purposes.	KCG Audit privacy notice Grant Thornton UK LLP privacy notice
Courts or Police forces or other agencies with responsibilities for the prevention and detection of crime, apprehension and prosecution of offenders or collection of a tax or duty, such as law enforcement or counter-fraud investigators, or for safeguarding.	Where applicable due to investigations or legal proceedings.	Kent Police privacy notice Action Fraud privacy notice National Crime Agency privacy notice Kent County Council privacy notices
Professional services	For professional advice purposes, including legal where necessary for the establishment, exercise or defence of legal claims.	See relevant organisation's privacy notice. E.g.Evershed's privacy notice Mills & Reeve privacy notice