

Privacy Notice for Staff

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

Version 1.3 – Updated March 2021

This privacy notice aims to communicate how we use your data in a concise manner in accordance with [GDPR \[1\]](#) 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 \[2\]](#) or by emailing dataprotection@kent.ac.uk.

Contents

Data Protection Register	2
Definitions	2
How we collect your information	2
The purposes of processing your information	3
Special Category Personal Data (including Criminal Data)	3
Who your information is shared with	4
Where in the world is your personal data transferred to?	6
How long do we keep your personal data for?	6
Your rights	6
Further processing of your data	9
Your obligations	9
SCHEDULE 1 – Categories of Personal Data	10
SCHEDULE 2 – HR Data Retention Schedule	13
SCHEDULE 3 – Purposes of Processing Personal Data	18
SCHEDULE 4 – Purposes of Processing Special Category Data	34

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>)

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 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

From time to time we may 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.

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 or for statistical purposes.

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.

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 European Economic Area, 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;
- we have put in place appropriate safeguards to protect your personal data, such as an appropriate contract with the recipient;
- 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, dependant on the retention period of the file that your personal data is held on.

Your rights

You have certain legal rights, which are briefly summarised below, in relation to any personal data about you which we hold.

Your right	What does it mean?	Limitations and conditions of your right
-------------------	---------------------------	---

<p>Right of access</p>	<p>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”).</p>	<p>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.</p>
<p>Right to data portability</p>	<p>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.</p>	<p>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.</p>
<p>Rights in relation to inaccurate personal or incomplete data</p>	<p>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.</p>	<p>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.</p>

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.

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.

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.

If you wish to exercise any of your rights please contact our Data Protection Officer at dataprotection@kent.ac.uk in the first instance.

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/>.

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 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.

SCHEDULE 1 – Categories of Personal Data

Type of personal data
a) Contact information
<ul style="list-style-type: none">• Name(s)• Known as names(s)• Address(es)• Email address(es)• Contact details including mobile telephone number(s)
b) Personal Information
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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 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

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 systems
- User IDs
- IP addresses

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

SCHEDULE 2 – HR Data Retention Schedule

Record type	Suggested retention period	Exceptions
<p>Recruitment documentation: employment/engagement application forms (including budget & authorisation documents).</p> <p>To also include: Advert, screen shots, shortlisting grid, interview notes for all unsuccessful resident shortlisted candidates, shortlisted applications, number and names of shortlisted candidates</p>	<p>For unsuccessful applicants: the data will be anonymised 1 year after the successful candidate commences engagement</p> <p>For successful candidates, 7 years following end of engagement</p>	<p>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:</p> <ul style="list-style-type: none"> • One year from the date sponsorships ends • The point at which a compliance officer has examined and approved them.
<p>References received during engagement process</p> <p>User accounts created by applicants during the hiring process</p>	<p>For unsuccessful applicants: the data will be anonymised 1 year after the successful candidate commences engagement</p> <p>For successful candidates: 7 years following end of engagement</p>	<p>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.</p>

	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	
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.

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				✓		

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

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

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
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	✓				✓	

