

## **STAFF PRIVACY NOTICE**

### **Purpose of this Notice**

This Notice explains how the University will collect and use staff personal data, how we share it, how long we keep it for and what your rights are in relation to it. For the purpose of this Notice “staff” includes employees, consultants, contractors, workers and those with honorary or visiting contracts.

The University is the data controller for personal data that we process about you.

Throughout this Notice, “University”, “we”, “our” and “us” refers to the University of Leeds of Leeds, LS2 9JT, “you” and “your” refers to any current or former member of University staff and to job applicants.

This notice does not form part of any contract of employment.

It is important that you read this privacy notice together with other applicable privacy notices.

### **Changes to this Notice**

We shall inform you of any changes to this Notice. This version is available at [http://www.leeds.ac.uk/secretariat/data\\_protection.html](http://www.leeds.ac.uk/secretariat/data_protection.html).

### **Anything you are not clear about**

If there is anything you are unclear about, please contact our Data Protection Officer, who shall be happy to answer any queries you may have concerning this Notice or the way in which we processes your personal data.

The Data Protection Officer's contact details are provided at the end of this Notice.

### **Where does the University get your personal data from?**

We obtain personal data about you from the following sources:

- from you e.g. when you apply to the University through your application form and recruitment process, then other information the University may collect through your job-related activities throughout your time working for us;
- from other University staff e.g. where internal references are sought
- from an external third party e.g. referees and checks for criminal records information or from an employment agency you may have used.

The provision of most data that you provide to us is a contractual requirement. If you do not provide us with information that you are contractually obliged to provide, the consequences will depend on the particular circumstances. In some cases we may not be able to provide you with certain services; in other cases, this could result in the termination of your contract.

### **Categories of personal data**

The University will collect and use your personal data to support its purposes described below. It is difficult to provide a definitive list of all the types of data you might share with us and that we might need to generate. However, the usual categories of personal data we expect to process about you include (but are not limited to):

- The contact details that you provide to us, including names, titles, addresses, telephone numbers and personal email addresses.
- Personal details/data such as date of birth, gender, etc.
- Family details such as next of kin and emergency contact information, details of any life assurance beneficiaries.
- National Insurance number.
- Lifestyle and social circumstances.
- Your position, role, contract terms, grade, salary, benefits and entitlements.
- Working hours, night workers assessment forms (where relevant), training records and if you leave, your reason for leaving.
- Records about your recruitment, including your application paperwork, details of your qualifications/education, references, requests for special arrangements, communications regarding our decisions, and relevant committee and panel reports.
- Copies of passports, driving licence and driving history, right to work documents, visas and other immigration data.
- Pensions membership data, including identification numbers, quotes and projections, terms benefits and contributions.

- Details of any medical issues and/or disabilities that you have notified to us, including any consideration and decision on reasonable adjustments made as a result.
- Equality monitoring data.
- Dietary requirements.
- Your financial details, including bank and building society account numbers, sort codes, BACS IDs, NI numbers, tax codes, payslips, payroll records, tax status information and similar data.
- Learning and development records, including your attendance, completions, accreditations and certifications.
- Capability procedure records, including performance indicators, records of review meetings, feedback, decisions and outcomes.
- Promotion and progression records, including applications, references and supporting materials, records of deliberations and decisions, feedback and awards.
- Records regarding grievances, disciplinary proceedings or investigations prompted by, involving or relating to you.
- Visual images, personal appearance and behaviour / photographs, audio and video recording (including CCTV).
- Absence records, including leave requests, sickness records and related data.
- Computing and email information, including login information for our IT systems, IP address(es), equipment allocated to you and records of network access.

The University may process so called “special categories” of personal data. These are more sensitive personal data which require a higher level of protection. This includes information relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, physical or mental health, or sexual orientation.

The University may also process information relating to any criminal offences or criminal proceedings. These are details of any relevant criminal convictions or charges that we ask you to declare to us, either when you apply to us, or during your employment. Relevant criminal convictions or charges are those that indicate you might pose an unacceptable risk to students or staff. Further, your role at the University may require that we conduct a Disclosure and Barring Service check, which will provide us with details of any relevant criminal convictions and/or cautions that you have received. More information is available here [http://hr.leeds.ac.uk/info/33/recruitment\\_and\\_redeployment/13/criminal\\_records](http://hr.leeds.ac.uk/info/33/recruitment_and_redeployment/13/criminal_records).

## **The purposes for which the University processes your personal data and the legal basis for that processing**

In general terms, the University will process your personal data for recruitment and employment related purposes.

The law requires that we provide you with information about the lawful basis on which we process your personal data, and for what purposes.

Most commonly, we will process your data on the following lawful grounds:

- To carry out our obligations under your employment contract with us.
- To administer your employee file including paying you or providing a benefit.
- To provide you with information about your employment.
- To manage sickness absence.

*Our lawful basis for the activities above is necessity to perform our employment contract with you.*

- Checking you are legally entitled to work in the UK.
- Ascertaining your fitness to work.

*Our lawful basis for the activities above is a necessity for the University to comply with its legal obligations.*

- At the end of your employment with the University for analysis of staff turnover.

*Our lawful basis for this activity above is the pursuit of our legitimate interests of recruiting individuals into the University as part of our business plan, provided your interests and fundamental rights do not override those interests.*

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

We may also use your personal information, typically in an emergency, where this is necessary to protect your vital interests, or someone else's vital interests. In a small number of cases where other lawful bases do not apply, we will process your data on the basis of your consent.

Data will be kept and used to allow the University to manage its relationship with you from the time of recruitment, to employment and for a time after your employment has ceased.

Please see table 1 for more information on the purposes for which we will process your personal data and the legal basis for that processing.

### **Additional notices and guidance/policies**

The University has also published separate policies and guidance which may be applicable to you in addition to other privacy notices. It is important that you read this privacy notice together with other applicable privacy notices.

The other relevant privacy notices include:

- Students
- Alumni
- Website and cookies

The relevant policies and guidance include:

- Use of computer systems. The University reserves the right in exceptional circumstances to monitor your use of its electronic systems e.g. your email. See [http://it.leeds.ac.uk/info/116/policies/260/use\\_of\\_computer\\_systems\\_policy](http://it.leeds.ac.uk/info/116/policies/260/use_of_computer_systems_policy)
- Audio visual policy. The University is committed to a lecture capture service which means that the University regularly records educational activities in which you may be involved. These recordings will be made in accordance with the University's policy on audio or video recording for educational purposes. Please note that under this policy you may opt out of recordings and request an edit of any recording made. Please see [http://www.leeds.ac.uk/secretariat/documents/audio\\_visual\\_policy.pdf](http://www.leeds.ac.uk/secretariat/documents/audio_visual_policy.pdf). Please read the policy to understand your rights and obligations. The University believes it has both a legitimate and public interest in pursuing the lecture capture service.
- Data protection. For more general information on the University's approach to data protection please see [http://www.leeds.ac.uk/secretariat/data\\_protection.html](http://www.leeds.ac.uk/secretariat/data_protection.html).

### **Who might we share your personal data with?**

As part of the University's normal business it will often need to share your personal information internally with other colleagues to carry out its day to day activities related to your job role and/ or to administer the working relationship with you. However, it is expected that this information is shared sensitively and on a "need to know" basis. Equally, sometimes the University will share some of your information externally with others e.g. including your details on University websites, promoting your and the University's activities. (For certain positions within the University it will be necessary to take up external references in order to achieve promotion.)

The University may also need to share your personal information with third parties where we are required to by law or there is a legitimate interest in doing so.

We do not, and will not, sell your data to third parties.

Sometimes to help us administer your contract of employment we will use third parties to help process your data (e.g. in relation to your pension fund). Where this is the case we will ensure that we have arrangements in place with these "processors" to ensure the safe use of the data.

Examples of bodies to whom we are required by law to disclose certain data include, but are not limited to:

<b>Organisation</b>	<b>Why?</b>
Home Office; UK Visas and Immigration	To fulfil the University's obligations as a visa sponsor
Disclosure and Barring Service (DBS)	Required for certain posts to assess an applicant's suitability for positions of trust or where the post works with vulnerable people or children.
Research England	Data submitted for the Research Excellence Framework (REF) which is a system for assessing the quality of research in higher education.
HM Revenues & Customs (HMRC)	Real time information released to HM Revenue & Customs (HMRC) in order to collect Income Tax and National Insurance contributions (NICs) from employees.

Examples of bodies to whom we may voluntarily disclose data, in appropriate circumstances, include but are not limited to:

Organisation	Why?
Agencies with responsibilities for the prevention and detection of crime, apprehension and prosecution of offenders, or collection of a tax or duty.	For the prevention, detection or investigation of crime, for the location and/or apprehension of offenders, for the protection of the public, and/or to support national interest.
Mortgage lender and letting agencies	In order to allow these organisations to verify for mortgages and tenancy agreements. Release of this information is subject to a written request being received from the employee.
Your pension scheme, eg, USS, NHS pensions, etc	In order to provide data required for the provision of pensions by these providers.
Higher Education Statistics Agency (HESA)	Some information, usually in pseudonymised form, will be sent to the HESA for statistical analysis and to allow government agencies to carry out their statutory functions.
Occupational Health providers	To enable the provision of these facilities.
Third party service providers	To facilitate activities of the University [including activities that are carried out by third-party service providers such as pension administration, benefits provision and administration and IT services]. Any transfer will be subject to an appropriate, formal agreement between the University and the third party service provider.

Table 1 has further information on where your data may be shared with third parties. Whenever we share your personal information with third parties we will continue to ensure this information is shared sensitively and on a “need to know” basis.

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes (as written in the contract between us) and in accordance with our instructions.

### Transfers to third party countries

Sometimes the University may need to share your personal data with other organisations based within or outside of the European Union. This may be required where you are conducting University business with that other organisation e.g. where you are seconded, or conducting research or teaching abroad.

The law provides various further safeguards where data is transferred outside of the EU.

When you are resident outside the EU in a country where there is no “adequacy decision” (a country outside the EU that ensures adequate level of data protection due to its domestic laws or international commitments) by the European Commission, and an alternative safeguard is not available, we may still transfer data about you which is necessary for performance of your contract with us .

Otherwise, we will not transfer your data outside the European Union without first notifying you of our intentions and of the safeguards that apply to your data.

### **Data security**

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business requirement to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from our IT Security Team (whom you can contact via the IT Service Desk) or from the Data Protection Officer (whose details are set out at the end of the document).

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

### **Retention periods**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use

or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of University we will retain and securely destroy your personal information in accordance with our Data Retention Policy.

We will retain your personal data as follows

- as long as it is necessary to fulfil the purposes related to your employment (see above) e.g. bank account information so we can pay you. We will keep most information relating to your personnel file (for example training records, your contract of employment, annual leave records, payroll and wage records) for the entirety of your employment and six years after.
- where we have to retain the data for legal reasons (including tax law, employment law, administrative law and other regulatory requirements) e.g. salary information relating to payment of tax .
- to address issues that may arise at a later date e.g. where you may need a reference or for audit purposes on a sponsored grant
- in most circumstances we will retain your personal data while their employment continues and for six years after it ends.

### **Your rights as a data subject**

We thought it would be helpful to set out your rights under the GDPR. You have the right to:

- withdraw consent at any time where that is the legal basis of our processing;
- access your personal data that we process;
- rectify inaccuracies in personal data that we hold about you;

- be forgotten, that is your details to be removed from systems that we use to process your personal data;
- restrict the processing in certain ways;
- obtain a copy of your data in a commonly used electronic form; and
- object to certain processing of your personal data by us.

Please be aware that these rights are subject to certain conditions and exceptions as set out in the data protection legislation.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, withdraw your consent to any processing, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing and they will explain any conditions that may apply.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Please see <https://ico.org.uk/> for further information on the above rights. You may also contact the Data Protection Officer for further information.

You have a right to complain to the Information Commissioner's Office about the way in which we process your personal data. Please see <https://ico.org.uk/>.

### **Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please inform your local Human Resources Manager if your personal information changes during your employment with us.

## Legal basis for processing your data under GDPR

Table 1 gives the University's present view on the grounds for processing against each specified purpose. We say "present view" as at the time of writing this the Data Protection Bill is yet to be finalised and there may be further guidance from the Information Commissioner's Office and/ or Article 29 Working Party about how these legal basis should be applied. This is in particular to which of our functions are a "public task" and which are in the "public interest". As legal views mature the University may change its views on its legal basis for processing.

Here is a brief explanation of the grounds referred to under table 1.

(Article 6(1)(a)), Consent – on specific occasions the University will only process certain data if you consent.

(Article 6 (1)(b)), necessary for the performance of your contract – on many occasions the University will process your data to enable it to meet its commitments to you e.g. necessary for the payment of your salary.

(Article 6 (1)(c)), necessary to comply with a legal obligation – the University does have legal obligations to provide your personal data to others e.g. necessary to complete tax records.

(Article 6 (1)(d)), for the purpose of protecting the vital interest of yourself or another – sometimes in extreme circumstances the University will have to release information to protect your interests or the interests of others e.g. in medical emergencies (such as when passing on personal details during a 999 call).

(Article 6 (1)(e)), processing necessary for the performance of a task carried in the public interest – the University is an educational establishment and in particular its educational activity is conducted in a public interest (including your interest and the interest of others).

(Article 6 (1)(f)), processing necessary for the purposes of the legitimate interest of the University or a third party subject to overridden interests of the data subject – the University (and sometimes third parties) has a broad legitimate interest in activities that connect to the activities of staff. Subject to those interests not being overridden by the interests of fundamental rights and freedoms of staff, it will pursue those interests.

In relation to special categories of data:

(Article 9(2)(a)), processing data where you have given consent – the University will process certain sensitive information about you with your consent.

(Article 9(2)(b)), processing data for the purposes of carrying out obligations and rights in the field of employment and social security and social protection law.

(Article 9(2)(c)), processing data necessary to protect your vital interests.

[(Article 9(2)(d)), processing carried out in the course of legitimate activities.

(Article 9(2)(e)), processing data made public by you.

(Article 9(2)(f)), processing “special categories” of data in connection with legal claims.

(Article 9(2)(g)), processing data where necessary for reasons of substantial public interest.

(Article 9(2)(h)), processing necessary for purposes of preventative or occupational medicine.

(Article 9(2)(i)), processing necessary for protecting public health.

(Article 9(2)(j)), processing for scientific or historical research purposes.

It is recognised that some of the above grounds will overlap and that the University could rely on multiple grounds justifying its lawful processing. The University also reserves the right to rely upon other grounds that are not referred to under table 1.

### **Concerns and contact details**

If you have any concerns with regard to the way your personal data is being processed or have a query with regard to this Notice, please contact our Data Protection Officer, David Wardle at [d.wardle@adm.leeds.ac.uk](mailto:d.wardle@adm.leeds.ac.uk).

Our general postal address is University of Leeds, Leeds LS2 9JT, UK.

Our postal address for data protection issues is University of Leeds, Room 11.72 EC Stoner Building, Leeds, LS2 9JT.

Our telephone number is +44 (0)113 2431751.

Our data controller registration number provided by the Information Commissioner's Office is Z553814X.

<b>TABLE 1</b>		
<b>No.</b>	<b>Specific Purposes</b>	<b>Legal Basis – reference to Article 6 GDPR unless indicated to the contrary</b>
1.	Payment of salary, pension, sickness benefit or other payments due under the contract of employment.	6(1)(b)
2.	Monitoring absence or sickness under an absence control or capability policy.	6(1)(b)  6(1)(c) [so far as it relates to statutory sick pay obligations]
3.	Training and development purposes.	6(1)(f)
4.	Management planning	6(1)(f)
5.	Providing and obtaining references - and consultation with external agencies including police checks where necessary for the purposes of employment - for job applicants and employees in post; and providing references for former employees.	6(1)(f)
6.	For disclosure to the police or other regulatory body where pursuant to the investigation or disclosure of a particular crime.	6(1)(f)  And provided a suitable condition is met under the Data Protection Act 2018, for example to prevent or detect unlawful acts, protecting the public against dishonesty and other improper conduct or for the purposes of compliance with regulatory requirements in certain cases. And further in each case, provided the relevant controls and conditions under the Act are met.
7.	Promotion and salary progression exercises.	6(1)(f)
8.	Negotiations with trade unions or other staff representatives.	6(1)(f)
9.	Curriculum planning and Organisation.	6(1)(e) and/or 6(1)(f)
10.	Time table Organisation.	6(1)(e) and/or 6(1)(f)

11.	Administration of University codes of practice and policies.	6(1)(e) and/or 6(1)(f)
12.	Compliance with equality legislation, including that relating to disability.	6(1)(c) and 9(2)(b)
13.	Compliance with any statutory or legal requirement to provide Information about staff or other workers including, for example, Statistical returns to external bodies and staff membership lists to Unions.	6(1)(c) and 9(2)(b)
14.	Administration of the University's disciplinary and grievance procedures.	6(1)(b) and 6(1)(f)
<b>No.</b>	<b>Specific Purposes</b>	<b>Legal Basis – reference to Article 6 GDPR unless indicated to the contrary</b>
15.	Direct mailing for third party Services reasonably concerned with employment- related matters or staff benefits.	6(1)(f)
16.	Production of published staff lists including the University Calendar and telephone and e-mail directories for both internal and external use.	6(1)(f)
17.	Production of Staff Identity Cards.	6(1)(f)
18.	Production of photographs of staff for display within the University or on the web (but see also paragraph 32 of the University's code of practice on data protection).	6(1)(f)
19.	Development of staff research profiles, intellectual property and knowledge transfer by associated University Companies.	6(1)(e) and/or 6(1)(f).
20.	Monitoring the use of University resources, including those provided by ISS (but see also paragraphs 33-37 of the University's code of practice on data protection). This may include accessing email accounts and data during unexpected staff absence and post employment (subject to formal authorisation and controls) that are intended to provide appropriate protection of your rights and freedoms).	6(1)(f)
21.	In relation to the safety of individuals and their property and the protection of University assets, including the use of CCTV.	6(1)(f)

		Where the processing involves data relating to potentially criminal behaviour, such processing is necessary for the purposes of the prevention or detection of an unlawful act, and is permitted under the Data Protection Act 2018, provided the relevant controls and conditions under the Act are met.
22.	In relation to the Provision of academic Services and other Services (for example, car parking).	6(1)(f)
23.	In relationship to membership of University and staff clubs, societies and similar organisations.	6(1)(f)
24.	For disclosure to close family and emergency Services in the event of an emergency, for example, illness, serious injury or bereavement, or the Police where pursuant to the investigation or disclosure of a potential crime	6(1)(f) and: <ul style="list-style-type: none"> <li>• 9(2)(c) where someone's life or health is in danger and the disclosure is necessary to protect that individual.</li> <li>• Where the processing involves data relating to potentially criminal behaviour, such processing is necessary for the purposes of the prevention or detection of an unlawful act, and is permitted under the Data Protection Act 2018, provided the relevant controls and conditions under the Act are met.</li> </ul> Otherwise under Art 9(2)(a), where we have your explicit consent to share information with your family/others
25.	In relation to exit questionnaires distributed to those leaving the University's employment.	6(1)(f)
26.	In connection with data processed by external contractors or Consultants from whom the University may obtain Services or seek advice subject to appropriate authorisation and controls that are intended to provide appropriate protection of your rights and freedoms.	6(1)(f)

No.	Specific Purposes	Legal Basis – reference to Article 6 GDPR unless indicated to the contrary
27.	For disclosure to Data Processors who are registered under the Data Protection Act in order for them to process data on behalf of the University for any of the purposes for which the University is permitted to process the data, including the Provision of academic and other Services by the University.	6(1)(f)
28.	For disclosure to the University’s insurers in respect of accidents occurring within the institution and to the University’s external auditors.	6(1)(f) and 9(2)(f), and/or in appropriate cases where such processing meets a condition under the Data Protection Act 2018 for example protecting the public against dishonesty and other improper conduct. And further, provided the relevant controls and conditions under the Act are met.
29.	The dissemination of staff contact details for use in connection with critical incident management plans.	6(1)(f)
30.	The disclosure to trade unions of University staffs’ names, staff category and relevant School/Service, as appropriate in serving good industrial relations.	6(1)(f)
31.	To professional bodies where registration is related to the contract of employment e.g. the GMC	6(1)(f)  And where special category and/or criminal allegations are involved: 9(2)(a), or provided a suitable condition is met under the Data Protection Act 2018, for example to prevent or detect unlawful acts, protecting the public against dishonesty and other improper conduct or for the purposes of compliance with regulatory requirements in certain cases. And further in each case, provided the relevant controls and conditions under the Act are met.

32.	Provision of support services, such as staff counselling and occupational health	6(1)(f)
33.	The granting of awards, such as the Long Service Award	6(1)(f)
34.	Processing and recovery of overpayments	6(1)(f)

