Leeds Beckett University Colleague Privacy Notice

WHAT IS THE PURPOSE OF THIS DOCUMENT?

Leeds Beckett University is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all employees, workers and contractors.

Leeds Beckett University is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, you will be notified of this the next time that you logon to Employee Self-Service. The updated version will also be published on the University’s main website.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

As a University we will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Driving licence and insurance details where you are required to drive on university business.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, job descriptions, work history, working hours, holiday and absence records, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- As part of our day-to-day measures to protect our university community we also collect CCTV footage and other location and engagement information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.
- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

- Information about criminal convictions and offences.

Most of this information is stored in our HR systems. However, some of the information such as CCTV footage and photographs is held in other University systems.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity, religion or belief and your sexual identify.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records, including:
    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
    - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees, workers and contractors through the application, recruitment and onboarding process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, the Disclosure & Barring Service (DBS) and the Home Office.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us. Much of the information that we collect can be checked and updated by you through our employee self-service system.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else’s interests).

2. Where it is needed in the public interest [or for official purposes].

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you [*] and to enable us to comply with legal obligations [**]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties [***], provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below. We have indicated by [asterisks] the purpose or purposes for which we are processing or will process your personal information, as well as indicating which categories of data are involved.

- *Making a decision about your recruitment or appointment.
- *Determining the terms on which you work for us.
- *Checking you are legally entitled to work in the UK.
- **Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- *Providing a range of staff benefits to you and giving you information about these benefits.
- **Enrolling you in a pension arrangement in accordance with our contractual and statutory automatic enrolment duties.
- **Liaising with our pension providers (NEST, Teachers' Pension Scheme, Universities Superannuation Scheme and West Yorkshire Pension Fund), any other provider of employee benefits.
- *Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- *Conducting performance reviews, managing performance and determining performance requirements.
- **Making decisions about salary reviews and compensation.
- *Assessing qualifications for a particular job or task, including decisions about promotions.
- *Gathering evidence for possible grievance or disciplinary hearings.
- *Making decisions about your continued employment or engagement.
- *Making arrangements for the termination of our working relationship.
- *Education, training and development requirements.
- **Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- *Ascertaining your fitness to work.
- *Managing sickness absence.
- **Complying with health and safety obligations.

- **To prevent fraud.
- ***To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- *To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- *To conduct data analytics studies to review and better understand employment trends and information about the profile of our workforce.
- *Equal opportunities monitoring.
- **Production of statistical returns required by certain third-party bodies, such as (but not exclusively) the Office for Students and the Higher Education Statistics Agency.
- ***Use of closed circuit television (CCTV) to protect students and employees and their belongings and university premises.
- *Administration of university policies, regulations, procedures and codes of practice as apply, and as notified, to staff.
- *Maintaining access to appropriate university systems.

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

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

”Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with employment.

3. Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.
- If you apply for an ill-health pension under a pension arrangement operated by the University, we will use information about your physical or mental health in reaching a decision about your entitlement.
- We will use information about your race or ethnicity, religion or belief and your sexual identify, to ensure meaningful equal opportunity monitoring and reporting, equality impact assessments, charter marks and other reporting including the provision of information to the Higher Education Statistics Agency.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.
- We may need to use special category information for the police or other regulatory bodies (including the Disclosure and Barring Service) in connection with the investigation or disclosure of a suspected or reported crime or the verification of identity.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about colleagues or former colleagues in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

We have a policy on Safeguarding Vulnerable Groups. Despite being primarily concerned with the delivery of higher education to adults, the University engages on a regular basis with both children and vulnerable adults. The Disclosure and Barring Policy sets out the approach that the University will take when recruiting employees and volunteers to posts involving work with children and/or vulnerable adults, including our legal obligations. The job description for the role sets out when a criminal record check is required and what level of check is needed.

If the post requires a criminal record check, we are required to carry out a check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role.

We are allowed to use your personal information in this way to carry out our obligations. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

DATA SHARING

We may have to share your data with third parties, including third-party service providers and other entities.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We will not transfer your personal information outside the European Economic Area unless an adequate level of protection for your rights and freedoms is available, or you give your express written consent for this to happen.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

”Third parties” includes third-party service providers (including contractors and designated agents) and other entities within our group. The following third-party service providers process personal information about you for the following purposes:

- The Office for Students and its Designated Data Body (currently the Higher Education Statistics Agency), Council Tax offices of local authorities, government departments or their agencies and other authorised users (including academic researchers, commercial organisations and survey contractors) for the creation, analysis and publication of staff statistics and/or to enable them to carry out their statutory or contractual functions as applicable, including those connected with higher education.
- Third parties that run pay surveys on the University’s behalf, such as UCEA and XpertHR, although the data is normally provided in an anonymised format.
- Emergency contacts and the emergency services where there is an emergency e.g. illness,

serious injury to staff or bereavement.

- Police, emergency services or other regulatory bodies (including the Disclosure & Barring Service and Home Office) in connection with the investigation or disclosure of a suspected or reported crime or the verification of identity.
- Our University's legal advisers and insurers for handling legal, regulatory and insurance cases, if and when they arise.
- Our University's auditors for official purposes.
- Third parties which undertake on our University's behalf the provision of learning and information services and IT support (including the provision of an email service for staff associated applications); specifically to Google for the provision of the Google Apps service; Microsoft for the provision of Office 365; and to Blackboard for the hosting of the MyBeckett platform.
- Suppliers that provide technical support for our University's HR information systems.
- HMRC, DWP, Courts and Councils for payroll purposes.
- Authorised benefit providers, usually to provide confirmation of the amount deducted through our payroll.
- Health service providers in order for them to provide the requested services to our staff.
- Atlantic Data to process DBS applications online.
- Third parties that provide specialist advice or guidance e.g. pension or benefit specialists.

We will share personal data regarding your participation in any pension arrangement operated on behalf of the University in connection with the administration of the arrangements.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group 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 and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example in the context of a TUPE arrangement or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC and disclosures to Governors such as senior staff remuneration reporting requirements.

Transferring information outside the EU

We will not transfer your personal information outside the European Economic Area unless an adequate level of protection for your rights and freedoms is available, or you give your express written consent for this to happen.

DATA SECURITY

We have put in place measures to protect the security of your information. Details of these measures are contained within our IT Security Policies that can be accessed on our website.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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 need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

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

DATA RETENTION

How long will you use my information for?

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. It will be kept in accordance with the records retention schedule which can be accessed at http://www.leedsbeckett.ac.uk/records-retention/. 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 the company we will retain and securely destroy your personal information in accordance with our data retention policy and applicable laws and regulations.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us. The main way to do so this is through our employee self-service system.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, the form for making Data Subject Access Request is available on the Data Protection page of the University's main website.

What we may need from you

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.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Human Resources by sending an email to hris@leedsbeckett.ac.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another

legitimate basis for doing so in law.

DATA PROTECTION OFFICER

We have appointed a Data Protection Officer to oversee compliance with this privacy notice. If you have any questions or concerns about how we handle your personal information, please contact the Data Protection Officer at: secretary@leedsbeckett.ac.uk in the first instance. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.]

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and you will be notified when we make any substantial changes the next time that you logon to our employee self-service system. You should also check for any updates that are published on the University's main website. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Human Resources in the first instance by sending an email to hris@leedsbeckett.ac.uk.

25 May 2018 v1