

# Privacy Notice for Brunel staff



## 1. About this Privacy Notice

As an employer, Brunel University London (we, us, our, 'the University') must collect and use personal data about our employees to ensure we meet our contractual and statutory obligations and can operate in line with our approved policies and procedures.

The University is a Data Controller, which means that we are responsible for deciding how we process personal information about you. We are registered with the Information Commissioner's Office (ICO) under the reference [Z6640381](#).

This Privacy Notice applies to all current and former staff, agency staff, contractors, work experience/placement students, affiliates, consultants, honorary appointment holders, interns or secondees, and any other person formally employed by the University.

It explains how we collect and use your personal data. However, the information we process about you will vary depending on your specific role and circumstances, and the University services with which you engage.

The following sections describe the usual ways we will process employee personal data. If we need to use your personal data in different ways, or for a different purpose, we will let you know, providing separate privacy information as required.

This Notice should be read in conjunction with other applicable privacy notices, such as our [General Privacy Notice](#), and our Data Protection Policy.

This Notice was last updated in April 2026

From time to time we update our Privacy Notice and any revised version will be made available on our website.

## 2. How we get your information

We get information about you from the following sources:

- Directly from you
- From an employment agency
- From your employer if you are a secondee or on placement
- From referees, either external or internal
- From security clearance providers, for example as part of a Disclosure and Barring Service 'DBS' check
- From Occupational Health and other health providers
- From pension administrators and other government departments, for example tax details from HMRC
- From your Trade Union
- From our Car Parking provider
- From providers of staff benefits
- From our CCTV systems

We collect other information about you as a result of your actions throughout the period of you working for us, for example, when you borrow a library book we create a record of your loans.

### **3. How we use your personal data**

As an employer we collect and use the following categories of personal data.

#### **3.1 Biographical information**

We use the following information to enter into and carry out the contract we have with you, and to manage our human resources processes.

- Employment and education history, including your qualifications, job application, CV, employment references, certificates, professional memberships, right to work information and details of any criminal convictions that you declare
- Personal contact details, such as your name, address, contact telephone numbers and personal email addresses
- Your date of birth, gender, and NI number
- A copy of your passport or similar photographic identification and / or proof of address documents
- Marital status
- University ID (for example, your staff number and photo)

We use your next of kin, emergency contacts and their contact information, for the purposes of protecting your vital interests. We advise you to notify the relevant person(s) that you are providing their contact details to the University as your listed contact.

#### **3.2 Information related to your salary, pension, and other financial arrangements**

We process this information for the payment of your salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or maternity leave.

- Information about your role and your employment contract, including:
  - your start and leave dates, salary (including grade and salary band),
  - any changes to your employment contract,
  - working pattern and location, including any requests for or arrangements relating to hybrid or flexible working
- Details of your working hours and any overtime, expenses or other payments claimed, including details of any loans
- Details of any leave including sick leave, holidays, special leave etc.
- Pension details, including contributions and beneficiaries, for the provision and administration of the relevant pension scheme
- Your bank account details, payroll records and tax status information
- National Insurance and other national identifier numbers to ensure you pay the correct National Insurance contributions
- Trade Union membership, for the purpose of the deduction of subscriptions directly from salary
- Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1 forms/matching certificates and any other relevant documentation relating to the nature of the leave you will be taking

#### **3.3 Information relating to your work, performance, and training**

We use this information to assess your performance, to provide you with access to services required for your role, to conduct pay and grading reviews, and to deal with any employer / employee related disputes. We also use it to meet the training and development needs required for your role.

- Information related to performance and progression, including probation reviews, proceedings relating to promotions and appraisals, and annual personal development reviews
- Details of workload and work allocation, staff organograms
- Records relating to the Higher Education Role Analysis (HERA) job evaluation scheme, where these refer to an individual role
- Records of work activities, such as reports, minutes of meetings, emails, research outputs, or recordings of lectures
- Records of work-related travel (for example, for conference or training purposes), including driver's licence details, where relevant to your role
- Grievance and dignity at work matters and investigations, including research misconduct investigations, to which you may be a party or witness.
- Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued
- Whistleblowing concerns raised by you, or to which you may be a party or witness
- Information related to your training history and development needs
- Higher Education Statistics Agency (HESA) statistics, required as part of our statutory reporting obligations
- Location of work, staff card (swipe) access details,
- Records of your access to and use of University IT services, including any personal data received or disclosed using the Brunel email system and any websites that you visit while logged on to a managed device
- Information about personal devices that you use to log in to our networks or systems including device information, your IP address, and information about how often you log on to our network
- Where relevant to your role, details of external funding applications, awards and agreements for research including postgraduate research, innovation and other externally funded activity

### **3.4 Information relating to your health and wellbeing and other 'special category' data**

We use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees.

- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e., Statement of Fitness for Work from your GP or hospital
- Accident records if you have an accident at work
- Details of any desk audits, access needs or reasonable adjustments
- Information you have provided regarding Protected Characteristics as defined by the Equality Act 2010 for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics
- Any information you provide to any of our equality and diversity networks

### **3.5 Information relating to monitoring**

We use this information to assess your compliance with University policies and procedures, for the prevention and detection of crime, and to ensure the security of our premises, IT systems and employees

- Information derived from monitoring IT acceptable use standards, in line with our policy <https://students.brunel.ac.uk/documents/Policies/Brunels-acceptable-computer-use-policy-2015.pdf>
- CCTV images and video footage

- All of our IT systems, and the swipe access system for the entry and exit of our premises are auditable and can be monitored, though we don't do so routinely

### **3.6 Other information**

- Any further personal information, such as academic qualifications or research output, or responses to staff surveys, that you have entered into a University system
- Information about your access to and use of University services, such as the Library or sports facilities, for the purpose of enabling your access to these services

## **4. Lawful basis for processing your personal data**

Depending on the activity, we rely on one or more of the following lawful bases for processing your personal data under the UK General Data Protection Regulation:

- Article 6(1)(b) which relates to processing necessary for the performance of a contract
- Article 6(1)(c) so we can comply with our legal obligations as your employer
- Article 6(1)(d) in order to protect your vital interests or those of another person
- Article 6(1)(e) for the performance of our public task
- Article 6(1)(f) for the purposes of our legitimate interest
- Article 9(2)(g) for processing necessary for reasons of substantial public interest

Please note, we will not request or rely on your consent as a lawful basis for processing your data as described in this Notice.

### **4.1 Special category data**

Where the information we process is 'special category' data<sup>1</sup>, the additional bases for processing that we rely on are:

- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent
- Article 9(2)(f) for the establishment, exercise or defence of legal claims
- Article 9(2)(j) for archiving purposes in the public interest, scientific or historical research or statistical purposes

In addition, we rely on the processing conditions in Schedule 1 of the Data Protection Act 2018.

- Part 1 paragraph 1, which relates to the processing of special category data for employment purposes.
- Part 1 paragraph 4, which relates to the processing of special category data for archiving, scientific or historical research purposes or statistical purposes.

---

<sup>1</sup> Special category data are personal data revealing or concerning racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); health; sex life, and sexual orientation

- Part 2 paragraph 8, which relates to the processing of special category data for equality of opportunity or treatment purposes.

#### 4.2 Criminal convictions and offences

We process information about staff criminal convictions and offences. The lawful basis we rely on to process this data is:

- Article 6(1)(b), which relates to processing necessary for the performance of a contract. Additionally, we rely on the processing condition at Schedule 1 part 1 paragraph 1 of the DPA.

### 5. How long we keep your information

We will keep your personal data only as long as is necessary for the purpose(s) for which it was collected. The retention periods for each purpose are set out in the University's Records Retention Schedules <https://www.staff.brunel.ac.uk/directorates/sas/library-services/record-management/retention-schedules>

### 6. Sharing your information

Your personal data will be shared internally between individuals and/or departments where this is necessary for the processing purposes set out above. For example, staff initially provide information to Human Resources when joining the University, but some information needs to be shared with our Information Services department to enable systems access and administration of Brunel IT accounts.

Depending on your role and circumstances, the University may also disclose certain personal data to external bodies, as named or categorised below. At all times, the amount of information disclosed and the manner in which it is disclosed will be in accordance with the provisions and obligations of UK data protection law.

We don't routinely transfer staff personal data overseas but when this is necessary we ensure that we have appropriate safeguards in place.

The organisations with whom we share data also have an obligation to tell you how they will use your information. We advise you to look at their privacy notices/policies.

Disclosure to	Nature of sharing
Higher Education Statistics Agency (HESA)	Information will be sent to the HESA for statistical analysis and to allow government agencies to carry out their statutory functions. Refer to the HESA staff collection notice for further details
HMRC	In connection with your pay, taxes, and benefits
Wholly Owned Subsidiaries of the University	In connection with contractual obligations
Banks and other financial institutions	In connection with your pay and benefits
Pensions providers	For providing and administering your pension

Occupational Health and other medical professionals	In relation to any medical condition, illness, or disability you may have or develop during the course of your employment
UK agencies with duties relating to the prevention and detections of crime, apprehension and prosecution of offender, collection of a tax or duty, or safeguarding national security (such as the Department of Work & Pensions or Police)	If requested, and only if sharing would be lawful
Professional bodies and regulators including regulatory bodies	For the independent evaluation, review, audit and investigation of individual and organisational activities and functions.
Other Universities, partners, project collaborators and funders, for outreach activity such for example: Medical School Council (“MSC”).	For the purposes of financial management and administration of a research contract or other projects and survey. Please note, you have the right to object to your personal data being provided to the MSC for the Clinical Academic Staff Survey.
Government agencies and public bodies, such as the Office for Students	In relation to submissions to research and teaching evaluation frameworks
Home Office, UK Visas and Immigration	To undertake Employer Checks, manage Certificates of Sponsorship and to comply with statutory monitoring and reporting requirements
Disclosure and Barring Service (DBS)	Required for certain sensitive posts to assess applicant’s suitability for positions of trust
Parking Management Provider	In relation to car parking access registration, parking tickets and removal

## 7. Automatic Decision Making, Profiling and AI use

Brunel University uses Microsoft Copilot Chat within our Microsoft 365 education environment. Staff can access this service using their Brunel IT account to ask questions and receive responses through a chat-based tool.

Staff are instructed not to enter personal data or sensitive information into Copilot Chat. However, we recognise that personal data may still be processed as part of generating responses.

For our teaching and learning activities, we rely on public task as our lawful basis. For any additional or incidental processing (such as system monitoring), we rely on legitimate interests and, where relevant, legal obligation.

AI is a tool to support our work and increasingly new and updated software will use AI to process data more efficiently. Each use of AI will be reviewed to ensure that it meets Data Protection requirements and where needed a Data Protection Impact Assessment will be required.

Any AI generated result will be accompanied by a statement that it was AI generated/processed using AI.

## 8. Data Processors

We also use third party organisations, known as data processors, to provide certain services on our behalf. In order to deliver these services, these organisations may have access to staff data. We are required to have contracts in place with each of these data processors. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will hold it securely and retain it for the period we instruct.

These data processors are primarily software providers, such as Quick Think Cloud Ltd (who provide CHIME), Microsoft (Office applications) and Unit4 Business World (used by Finance, HR and Payroll). For further details of the data processors used, please contact the data protection team in the first instance.

## 9. Your rights

Under data protection law, everyone has the following rights:

- **The right of access to your data** - You have the right to ask us for copies of your personal data
- **The right to rectification** - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete
- **The right to erasure** - You have the right to ask us to erase your personal information in certain circumstances
- **The right to restrict processing** - You have the right to ask us to restrict the processing of your personal information in certain circumstances
- **The right to object to processing** - You have the right to object to the processing of your personal information in certain circumstances
- **The right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances
- **Rights in relation to automated decision making and profiling**

For more information on your data protection rights, who to contact if you want to make a request or have a complaint or concern about the accuracy, retention or processing of your personal information, please contact [data-protection@brunel.ac.uk](mailto:data-protection@brunel.ac.uk).

You can also complain to the ICO if you are unhappy with how we have used your data. You can do this by visiting <https://ico.org.uk/for-the-public/how-to-make-a-data-protection-complaint/>.

## Document properties

<b>Author</b>	<b>Lorna Goodey</b> , Head of Privacy & Data Protection Officer (DPO)
<b>Approved by</b>	<b>Information Assurance Committee</b>
<b>Version</b>	1.0
<b>Classification</b>	Unclassified
<b>Date effective</b>	April 2026
<b>Previous review date</b>	April 2024

<b>Future review date</b>	April 2028
<b>Applicable law</b>	UK General Data Protection Regulation and Data Protection Act 2018