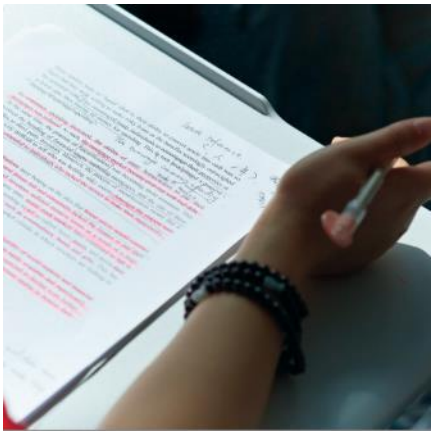
UNIVERSITY of BRADFORD

Data Protection

Privacy Notice for Staff Personal Data



Version Control

Notice Number:	
Approved by:	
Date Approved:	
Next Review Date:	
Version Number:	1
Applicable Statutory, Legal or National Best Practice Requirements:	General Data Protection Regulations and Data Protection Act 2018

This document can only be considered valid when viewed via the University website. If thisdocument is printed into hard copy or saved to another location you must check that the versionnumber on your copy matches that of the one on the University website. Approved documents are validfor use after their approval date and remain in force beyond any expiry of their review date untila new version is available.

1. Introduction

In order to comply with its obligations, the University of Bradford is required to process the personal data of its members of staff. In the main these obligations relate to the exercise of the contract of employment but also relate to the University's legal obligations and public functions.

This processing includes special categories of personal data which are discussed below.

All such data will be processed in accordance with the provisions of the General Data Protection Regulation and Data Protection Act 2018 (GDPR).

GDPR is a Data Protection law that applies across the EU and to all processing of personal data relating to EU citizens. The Data Protection Act 2018 supplements GDPR by making provision for those areas that GDPR left to national governments to determine, implements the EU's Law Enforcement Directive and extends data protection laws in other areas.

The UK has committed to continue to adhere to the GDPR after the University has left the European Union.

2. What is personal data

Personal data is information relating to an identified or identifiable living person (these are called data subjects) who can be identified directly or indirectly.

2.1. Special categories personal data

There is a further group of personal data described as special category personal data. This includes information relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs or trade union membership;
- Genetic or biometric data used for the purpose of identification;
- Health;
- Sex life or sexual orientation.

Specific arrangements exist for the processing of these types of personal data and these are described in section 8.1.

2.2. Personal data relating to criminal convictions and offences

Personal data relating to criminal convictions and offences or related security measures is another category of personal data which has specific rules for its processing.

Specific arrangements exist for the processing of these types of personal data and these are described in section 8.1.

3. Purposes for which personal data will be used

3.1. Job applicants

Personal data provided by job applicants and their referees will be used within the University to process those applications.

3.2. Members of Staff

Personal information relating to members of staff will be used for the purposes of employment, i.e. the exercise of the performance of the contract of employment.

This includes:

- Recruitment;
- Onboarding and induction;
- Employee administration;
- Provision of employment services;
- Access to the ICT and other facilities required for members of staff to do their jobs;
- Training and development;
- Provision of salary, expense payments, performance recognition, bonuses and pay awards;
- Health and safety;
- Employee relations processes e.g. discipline, dignity and respect, grievance, capability, attendance management, organisational transformation, employment tribunals etc;
- Reporting to external bodies on our activities.

Personal information relating to members of staff will also be used when you voluntarily choose to access any University benefits e.g. childcare vouchers, cycle to work scheme etc. Your decision to voluntary access these schemes is taken as authorisation for the University to process any of personal data required.

Activities such as counselling, medical care, nursery, sports centre may use the personal data held centrally by the University for activities associated with the above functions but separate privacy notices will explain to you how these activities process your personal data.

Any personal data we hold will not be excessive nor will it be shared more broadly than it needs to be.

4. What personal data do we use?

The personal data held about members of staff may include:

- Employee number;
- Name, address and other basic personal contact details;
- Date of birth;
- Nationality, country of birth, country of domicile;
- Passport/visa information;
- Bank details;
- Education details;
- Employment details;
- Employee relations records;
- Visual images, personal appearance; and
- Information relating to your activity.

In addition to this, the University may process some special categories of personal data about you such as:

- Racial and ethnic origin;
- Sexual orientation;
- Religious or other similar beliefs;
- Disability status and physical & mental health details;
- Offences and alleged offences;
- Criminal proceedings, outcomes and sentences;
- Information relating to Disability and Barring Service (DBS) checks.

5. Where the University gets its information from

The data held by the University is mainly taken from the details you provide as part of your job application and subsequently, when you update your personal information via MyView, from referees and former employers and education providers, from your line manager and other members of staff.

This may include special categories of personal data (which is explained below) and include photographs. Other information may be received from some of the bodies listed in the Appendix 1.

6. Sharing personal data (third party disclosures)

The University may disclose appropriate personal data, including special categories of personal data, to third parties, where it is appropriate to do so e.g. prospective employers, employment tribunals, external auditors, police forces, legal representatives etc.

Such disclosure is subject to procedures to ensure the identity and legitimacy of such organisations and their processing. A list of typical organisations the University may share information and further details on sharing to these organisations can be found in the Appendix 1.

7. Do we transfer the information overseas?

Data relating to specific members of staff may be transferred overseas to University staff based in the University of Bradford Regional Hubs in Beijing, China and Dubai to process applications from international students in that region. Information provided to the Regional Hubs will be subject to the same protection, processes and rights as data held in the UK.

8. Under what legal basis do we process your personal data?

In order to process personal information, the University must have a legal basis to process the information. In most cases, the University will process applicants and members of staff's personal data because it is necessary for the performance of the contract of employment or in order to take steps prior to entering into this.

For applicants who have applied for a job, the University needs to use your data as the first steps towards potentially offering you a job.

If you are employed as a member of staff the University needs to use your data to perform its obligations under the contract of employment.

There will be cases where there are other legal bases. For example:

- The University shares information with the police where the request is appropriately authorised and processing is necessary for the performance of a task carried out in the public interest;
- It may share information with medical services under the vital interests where there are grave concerns relating to a staff member's health and wellbeing;
- It shares information with the Higher Education Standards Agency (HESA) and UK Visas and Immigration (UKVI) as it has a legal obligation to do so.

There will also be situations where the University will process data for the purposes of the legitimate interests pursued by the University or by a third party. Where the University relies on legitimate interests, it must only do so where these interests are not overridden by the interests or fundamental rights and freedoms of the individuals concerned.

8.1. Special categories of personal data and data relating to criminal convictions.

There are additional requirements where the University processes special categories of personal data and data relating to criminal convictions.

The University collects and processes such information in order to undertake equal opportunities monitoring.

In most other cases, the University will only process special categories of personal data where it has explicit consent to do so.

This data will only be accessed by who have a legitimate need to see it.

8.2. Data relating to criminal convictions.

We also ask in some situations that applicants and members of staff provide information relating to any criminal convictions so that a decision can be made on whether we can offer a job.

Also, for certain roles relating to activity accredited by professional, regulatory or statutory bodies, the University is legally required to collect and process data on past criminal convictions.

In most cases the University will only process data relating to criminal convictions where it has explicit consent to do so or where processing takes place under its official authority.

9. How long is personal data retained by the University

Personal data will generally be retained for six years after the end of a staff member's employment at the University. There are a number of exceptions:

- Certain medical information must be retained for longer periods;
- Records of grievances, disciplinary matters etc. are retained for six years after the closure of the case;
- A core record to demonstrate and verify your employment at the University is retained for every member of staff permanently;
- For those who apply for a position at the University but are not appointed, their personal data will be held for 6 months after the end of the recruitment exercise.

To access the University's Retention and Disposal Policy which sets out the length of time that the University's records are retained please follow this link: https://www.bradford.ac.uk/publication-scheme/media/publicationscheme/policies/FINALretentionschedulerevisedMarch14.docx

10. Your rights

As a person whose personal data we are processing, you have certain rights in respect of that personal data; you have the right:

- To access your personal data that we process;
- To rectify inaccuracies in personal data that we hold about you if it is inaccurate or incomplete;
- To request the deletion or removal of your personal data where there is no compelling reason for its continued processing;
- To restrict the processing of your personal data in certain ways;
- To obtain your personal data for reuse;
- To object certain processing of your personal data;
- To complain to the Information Commissioner's Office about the way in which we process your personal data.

If you want to look at and check the accuracy of the personal data held by the Human Resources Service you should in the first instance request informal access to that information.

If you wish to formally access your personal data you should make a Subject Access Request. For more details please refer to the website: https://www.bradford.ac.uk/data-protection

11. Providing personal data to the University

Staff must ensure that all personal information provided to the University is accurate and up to date.

You should notify the University of any changes of address, corrections to contact details etc. by updating your personal information via MyView.

12. Complaints

If you believe that any part of the University is not complying with GDPR, the Data Protection Act 2018 or its own Data Protection Policy, you have the right complain to the University's Data Protection Officer.

Complaints should be submitted to the Data Protection Officer, email: data-protection@bradford.ac.uk

If you do not wish to contact the University or are not content with the outcome of its internal processes, you have the right to complain directly to the Information Commissioner's Office (ICO):
ICO
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113

Appendix 1 - Details of Information Sharing

The University's partners and contractors

The University may provide personal information to its partners and contractors. In such cases, the University must ensure that this information is managed in accordance with the GDPR, under contractual or similar arrangements and only for the purpose(s) for which it was provided to the partner/contractor.

Office for Students, the Quality Assurance Agency, Higher Education Statistics Agency (HESA), Office of the Independent Adjudicator and other HE bodies

Your personal data will be provided to the above bodies etc. in accordance with the regulations in place and the University's statutory obligations.

Further details about the data shared with HESA can be found in the HESA Staff Collection Notice on the HESA website.

References

The University will routinely provide a basic employment reference for members of staff.

Police, crime and taxation

The University may be informed by the Police when members of staff are convicted or cautioned etc.

The University may also provide information to the Police or other organisations that have a crime prevention or law enforcement function, such as benefit fraud departments of Local Authorities, about members of staff if it is necessary for the prevention or detection of a crime or the collection of taxes etc.

CCTV

The University has a CCTV system across its estate. Cameras located on and within buildings are monitored by trained security staff. All staff operating the CCTV system do so in compliance with GDPR, the Data Protection Act 2018, the 2008 CCTV Code of Practice, the Regulation of Investigatory Powers Act 2000 and the Private Security Industry Act 2001 and the University's Data Protection Policy.

Professional Bodies

Personal data relating to staff working on specific programmes will be passed to professional bodies which accredit those programmes at the University, those with a regulatory function over our programmes or where qualification on a programme facilitates membership or registration of that body.

Government bodies and NGOs

Many government bodies and NGOs have statutory powers to require the University to provide personal information. This includes UK Visa and Immigration, a subsection of the Home Office.

Others may request information relating to their official functions and the University will normally provide the information requested if it is deemed appropriate to do so.

Court Orders

Where a court orders the University to release information, it has a legal obligation to do so.

Solicitors

The University receives requests for personal data from solicitors acting on behalf of a member of staff party. In such cases, before any personal data is disclosed, the University requires the solicitor to provide consent from the member of staff to demonstrate that they are acting on their behalf. Solicitors often refer to this as a form of authority.

In rare cases where a solicitor acting on the other side of a legal case requests information, information will only be provided where the University receives consent or a court order.