

# Bangor University: Privacy Notice for Staff 2020/21



## 1. Introduction

Bangor University (BU) is the data controller in relation to your information, as defined in the Data Protection Act 2018 and is committed to protecting your rights, in line with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

The University's nominated representative for data protection legislation, and the Data Protection Officer is:

Head of Governance and Compliance  
Governance and Compliance Office  
Corporate Services  
Bangor University  
College Road  
Bangor  
Gwynedd LL57 2DG

This statement explains how the University handles and uses your personal information during your time at Bangor as a member of staff. The University is committed to protecting your personal information and to being transparent about what information it holds. The University has a range of data protection related policies and procedures in place which can be found here:

<https://www.bangor.ac.uk/governance-and-compliance/dataprotection/index.php.en>

## 2. What information do we collect about you?

BU will collect information about you throughout its dealings with you as a prospective and current member of staff. We will keep a record of the details you provided on your application form (or equivalent), any supporting documents we request as part of the recruitment and selection process, additional details provided by any referees and records following any interview process.

The types of personal information processed include, though is not limited to, the following:

### **Applicant Data**

- All documentation you provide to us a part of the application process.
- References received from your named referees as part of the application process.
- Records of the recruitment and selection process including any records following the interview process. As detailed in our Recruitment & Selection Collection Notice, the information you give us will be kept confidential, will be shared strictly in

accordance with the requirements of recruitment and selection, and your personal information will not be disclosed to third parties without your prior consent except where necessary to confirm factual information provided by you.

- Personal data of unsuccessful candidates will be deleted after a period of 12 months unless otherwise instructed or required for legislative purposes. If you are successful, the information is retained and transferred to your confidential staff record.

### **Staff Data**

- Your name, address and contact details, any telephone numbers you provide us with, date of birth and gender.
- Details of your qualifications, skills, experience and employment history, including start and end dates with previous employers and within the University.
- Salary information, pay progression and awards, pension information.
- Details of your bank account and national insurance number.
- Information about your nationality and entitlement to work in the UK documentation.
- Your emergency contact details if provided by you.
- Any applications for promotion/re-grading which you have submitted or have been submitted on your behalf by your manager together with any references received as part of this process.
- Details of periods of leave taken by you, including holiday\*, sickness absence, family leave, special leave and study leave\*.
- Information gathered for the purposes of equal opportunities monitoring (e.g. ethnic origin, sexual orientation, religious beliefs, disability information). Any reports/returns produced using this type of data will be anonymised.
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.
- Your PDR record\*.
- Your staff development record – details of training you have participated in and contractual development requirements (e.g. PGCert HE, Welsh Language courses)
- Your confidential occupational health record.
- For certain roles information about past criminal convictions may be processed as detailed under our DBS Policy.
- Information related to the prevention and detection of crime and the safety and security of staff and students, including, but not limited to, CCTV recording and data relating to breaches of University regulations.

\* Holiday, Study leave and PDR records are maintained within your School or Department

Some of this data may be categorized as special categories data, as defined by the Data Protection Act 2018.

### **3. How will your information be used?**

It is not possible to state every purpose for which your information will be used by BU however, in most cases, your personal information is either necessary for the performance of our contractual obligations with you or necessary for compliance with a legal obligation e.g Eligibility to Work in the U.K, Real time Information (RTI), Equality Act 2010 and The Equality Act 2010 (Statutory Duties) (Wales) Regulations 2011.

It may also be required in order that we may fulfil tasks required in the public interest e.g. HESA reporting (detailed in your contract of employment) and, for certain positions, to carry out criminal record checks - Disclosure & Baring Service checks (DBS).

The following are examples of how information is likely to be used:

- To assess your suitability for a role.
- To undertake pre-employment right to work checks and, for visa nationals, continuation of employment checks.
- To administer payroll, pension and other standard employment functions.
- To ensure effective HR and business administration
- To deliver facilities, services and benefits to you, and where appropriate, to monitor your use in line with University policies e.g. Acceptable Usage of IT Services.
- To communicate effectively with you by post, email and phone.
- To support your development, training, safety and wellbeing requirements.
- To fulfil and monitor our requirements under the Equality Act 2010 and The Equality Act 2010 (Statutory Duties) (Wales) Regulations 2011.
- To obtain Occupational Health advice to ensure we comply with our duties in relation to individual health conditions, meet our obligations under Health & Safety law.
- To ensure you receive pay, or other benefits, to which you are entitled to.
- To ensure we comply with our responsibilities under public safety legislation.
- Where relevant, to monitor, evaluate and support your research and enterprise activity.
- To enable us to contact others in the event of an emergency - If you have provided us with this information we understand that you have done so having obtained the named person's permission before sharing their details with us.
- To compile statistics and conduct surveys and research for internal and statutory reporting purposes (e.g. Higher Education Statistics Agency (HESA)).
- To respond to statutory requires (e.g. Benefits Agency as required by the Social Security Administration Act 1992)
- To share information with Public Health Wales in relation to the notification of notifiable infectious diseases.

### **4. Who receives your information?**

The Human Resources Team, Payroll and Pensions, have access to your personal data and are responsible for maintaining your personal file and records on the HR system.

Other colleagues, including your Head of Department/College/School and, where appropriate, line manager and departmental administrators, Finance (including Research), Planning and limited IT Services staff will have limited access to your records as necessary to perform their duties and business tasks.

Where necessary, personal information will be shared internally between academic and professional service departments across the University and, in relation to particular processes, such as investigations or appeal panels, other senior University staff/members of Council. Information will not be disclosed to third parties without your consent, or, unless it is permitted by law or contract.

This section outlines the major organisations and the most common circumstances in which the University discloses information about its staff. Where this involves international transfer, information will only be transferred if it meets the conditions outlined in the Data Protection Act 2018.

- The external providers of staff benefits including USS and BUPAS.
- Higher Education Statistics Agency (HESA) - BU is required to send some of the information which we collect about you to HESA for statistical analysis purposes. Details relating to the processing of your personal data by the Higher Education Statistics Agency can be found here: <https://www.hesa.ac.uk/about/regulation/data-protection/notices>
- Prospective and actual research funders or sponsors. This may include providing personal information for a Research Passport.
- The University is licensed to sponsor migrant staff under Tier 2 and Tier 5 of the points-based system. The University will provide data about staff on the Tier 2 and Tier 5 Visas to the Home Office and its departments in order to fulfil its duties under its license.
- Relevant Government Departments including HMRC and UK Visa and Immigration (UKVI)
- The Higher Education Funding Council Wales (HEFCW) in line with our statutory responsibilities.
- Any relevant simultaneous employers e.g. NHS Trust, Knowledge Exchange Partners
- Where you have given permission for information to be shared with relevant Trades Unions and external enquirers (e.g. a bank for mortgage reference, letting agencies, your solicitor for recovery of salary in injury claims).
- UK agencies with duties relating to prevention and detection of crime, collection of a tax or duty or safeguarding national security. You should note that there is a statutory duty for higher education institutions to have due regard to the need to prevent individuals from being drawn into terrorism. This may mean that, in particular circumstances, the University will need to pass on personal data to coordinating bodies and partner organisations such as local government and the police. Also courts or Coroners' Offices.
- Auditors, solicitors, insurers and other agents of the University may require access to personal data from time to time where this becomes necessary. These decisions

will always be made on a case by case basis by the Head of Governance and Compliance.

- On occasion and where necessary, debt recovery and control companies in order to recover debt on behalf of the University, where internal debt recovery procedures have been unsuccessful.
- On occasion, where necessary and where you have given permission, to medical practitioners to obtain Occupational Health advice to ensure we comply with our duties in relation to individual health conditions.
- Public Health Wales in relation to the notification of infectious diseases.
- NHS Wales Test, Trace and Protect Service to support the contact tracing process under Covid-19 regulations, when required.
- Any other disclosures that the University makes will be in accordance with data protection legislation and your interests and rights will be carefully considered.

Your basic contact details and role appear on our online directory. Separately, Schools and Departments may request you to provide other information for their webpages.

Staff working in customer or 'front-facing' positions may be expected to wear name badges as appropriate and may also have their names displayed on till receipts. Names and photographs may also be displayed on Department and School noticeboards.

## **5. Further information relating to your**

### **data**

#### **Your rights**

You have a right to access your personal information, to object to the processing of your personal information, to rectify, to erase, to restrict and to port your personal information. If you have provided consent to BU to process any of your data then you also have a right to withdraw that consent. Please visit the University Data Protection webpages for further information in relation to your rights:

<https://www.bangor.ac.uk/governance-and-compliance/dataprotection/index.php.en> Any requests or objections should be made in writing to the University Data Protection Officer.

#### **Security**

Data protection legislation requires us to keep your information secure. This means that your confidentiality will be respected, and all appropriate measures will be taken to prevent unauthorised access and disclosure. Only members of staff who need access to relevant parts or all of your information will be authorised to do so. Information about you in electronic form will be subject to password and other security restrictions, and paper files will be stored in secure areas with controlled access. Further information on these processes can be found in the University's *Information Security Policy*.

## **Retention**

The University retains your information in line with established higher education retention schedules. Further information can be found in the University's retention schedule which can be accessed here:

<https://www.bangor.ac.uk/governance-and-compliance/records-management.php.en>

## **Complaints**

If you are unhappy with the way in which your personal information has been processed you may, in the first instance, contact the University Data Protection Officer using the contact details above.

If you remain dissatisfied then you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: -

The Information Commissioner 2<sup>nd</sup>  
Floor  
Churchill House  
Churchill Way Cardiff  
CF10 2HH  
Tel: 02920 678 400

## **Your responsibilities**

You have a responsibility to keep your personal details up-to-date. During the course of your employment there are a number of circumstances in which you may have access to personal information about others, either at BU or elsewhere, such as at a work placement. You are expected to treat this in a responsible and professional manner and are legally required to do this under data protection legislation, as well as any professional ethics, codes of conduct or local rules and regulations. If you are made aware of personal information in confidence you are expected not to disclose this information to anyone without that individual's consent, unless there are exceptional circumstances. You should also not seek to gain others' personal data if you are not entitled to it. Disciplinary action will be considered for any University member of staff who breaches data protection legislation or a duty of confidence.

For further information consult the University's *Data Protection Policy*.

*Reviewed by the Head of Governance and Compliance  
for the 2020/21 academic year  
September 2020  
Approved by the Compliance Task Group 16<sup>th</sup> October 2020*