**BU Privacy Notice: Workforce and Applicants**

In this Notice:



## 1. Introduction

In this Notice, “BU” "we", "our" and "us" refers to Bournemouth University Higher Education Corporation.

As an employer BU must meet its contractual, statutory and administrative obligations. We are committed to ensuring that the personal data of our staff and applicants is handled in accordance with the principles set out in our Data Protection Policy and Key Data Protection responsibilities for BU Staff.

This Notice tells you what to expect when BU collects personal information about you. It applies to all employees, former BU staff and spouses who are in receipt of pensions, agency staff, volunteers, staff related visitors (such as academic collaborators, external examiners), contractors, secondees, honorary individuals and BU Board and subsidiary company Board members and applicants or proposed appointees for the same. However, the information we will process about you will vary depending on your specific relationship with us, such as your role or contractual status and personal circumstances.

Where we hold information in a form that identifies individuals, it is “personal data”, often referred to as “data” in this Notice. BU is the controller for this information unless this Notice specifically states otherwise. BU’s Data Protection Officer (“DPO”) has oversight over data protection matters within BU. If you have any questions about this Notice, or any queries or comments on the processing described in this Notice, you can contact the DPO on dpo@bournemouth.ac.uk**,** +44 (0) 1202 962472 or Poole House, Bournemouth University, Fern Barrow, Poole BH12 5BB.

From time to time, we will make changes to this Notice. Significant changes will be notified to you using our main or most common method of communication with you. For current staff, we will communicate these changes to you via email and by posting a news item on the staff intranet. For current job applicants, significant changes will be notified to you via email. For former staff, then significant changes will be notified by email or, if we do not have an email address for you, by writing to you at your residential address.

This Notice should be read in conjunction with our Data Protection Policy, Key Data Protection responsibilities for BU Staff and our other relevant policies and procedures. When appropriate we will provide a ‘just in time’ notice to cover any additional processing activities not mentioned in this document.

Please tell us promptly about any changes to the data we hold about you. This is particularly important for your contact details.

Current staff can do this through myHR (also referred to as the Employee Self Service Portal (ESSP)). myHR allows you to make some changes to personal details, view absence records, view, download and print your payslips and P60s, update your bank account details for payroll and view your employment information. For any other changes to your personal details, please email them through to HREnquiries@bournemouth.ac.uk.

For current job applicants, please update your contact details via our online recruitment system, Eploy.

## 2. When and how we collect your data

We get information about you from the following sources:

- Directly from you, including Application Form and Equality Monitoring Forms for our employee applicants.
- Directly from you in response to competitions or similar scenarios.
- From an employment agency.
- From your employer if you are a secondee or a contractor.
- From people you identify as referees.
- From third parties, such as the Disclosure and Barring Service, the Higher Education Statistics Agency, the UK Visas and Immigration service (part of the Home Office).
- 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 the Car Parking Scheme.
- From providers of staff benefits.
- CCTV footage and other electronic records such as smartcard technology.

## 3. What personal data we process and why

**Information related to your application and role**

We use the following information to carry out recruitment and selection processes. If appointed, you will provide and BU will receive data about you in respect of the work you undertake for us and your communications with BU staff, students and other individuals as part of your role at BU, and we will use this information for all purposes associated with the administration of your role. In addition, we use this information for the purpose of:

- providing opportunities under the guaranteed interview scheme for applicants who meet the minimum requirements and declare a disability.
- contractual administration.
- providing support services.
- IT and other systems access.
- managing compliance with legal requirements.
- statutory returns and compliance (such as monitoring equal opportunities and equal / gender pay, and processing and responding to subject access requests and information requests and complying with our obligations under our publication scheme).
- carrying out research, surveys and statistical analysis (including using third party data processors to carry out benchmarking and surveys for us).
- safeguarding and promoting the welfare of staff, students and visitors.
- ensuring the safety and security of our staff, , students and visitors.
- preventing and detecting crime.
- dealing with complaints and carrying out audits.
- supporting staff with making applications for research or other funding and regulatory approvals.
- business continuity and emergency purposes.

The data we collect about you includes:

- Applicant information (including your name, title, addresses, telephone number(s), and personal email addresses, employment and education history, details of any criminal convictions that you declare, copies of right to work documentation, references and other information included in your application form, Equality Monitoring forms, a CV or cover letter or as part of the application process).
- Shortlisted applicant information such as test and assessment performance and interview notes.
- Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses.
- Your date of birth, nationality, ethnicity, religion or belief, sexual orientation, legal sex, sexual orientation, if your gender is the same as your sex registered at birth, disability, and National Insurance number.

- For HMRC compliance, BU is obligated to maintain an employee's complete legal name, date of birth, gender (legal sex), full address, and national insurance number. Additionally, BU requires your tax code and student loan information, typically acquired from your P45 form.
- A copy of your highest and/or relevant educational qualification(s) and/or professional membership(s).
- Your photograph for the purpose of production of an access card.
- Bank details and information about your tax status and pension.
- Continuous service date if different to your start date with BU.
- A copy of your passport or similar right to work documentation.
- Marital status.
- Your emergency contacts and their contact information.
- HESA Identification Number (if previously employed by a Higher Education Institution).
- Teachers Reference Number if applicable.
- Conflict of interest declarations or gift declarations.
- Your responses to staff surveys if this data is not anonymised.
- Information relating to your salary, annual leave, pension, benefits and any other payments between you and us.
- If you drive a vehicle on BU business, a record of you having a valid driving licence and business insurance cover.
- Employment records (including job titles, work history, working hours, variations to terms and conditions, flexi-time, leave, sabbaticals, academic study leave, career breaks, paternity, maternity, adoption and other family leave, training records - including details of whether you have completed mandatory BU training and any professional memberships).
- Pension details including membership of occupational pension schemes (current and previous).
- Information relating to your performance and training. We use this information to assess your performance, undertake appraisal and to deal with any disputes and complaints. We also use it to meet the training and development needs required for your role.
- Information relating to your performance at work e.g. probation reviews, personal development plans, pay progression applications, promotions.
- Audio or video recording of lectures, presentations or training events, such as Panopto lecture capture system. Meetings may be recorded where there is a need for reasonable adjustments (see Accessibility Guidance) and agreement from the attendees.
- Information relating to any matters or complaints raised and investigated under BU policies and procedures, such as the Absence Management Policy, Dignity and Respect (Harassment) Policy, Disciplinary Procedure, Grievance Procedure, Sexual Harassment and Sexual Misconduct Policy and Performance Framework (Support and Development).
- Whistleblowing concerns raised by you, or to which you may be a party or witness.
- Your communications with BU staff, BU students and other people (including any opinions about you or made by you about another person).
- When you leave BU, your leaving date and your reason for leaving including any notes from the exit interview.
- Any Settlement Agreement which may be in place with regard to your employment.
- Redundancy information.
- Dismissal information.
- Details of any request you make to us and our handling of it, such as under the Freedom of Information Act 2000 or under the data protection laws.
- Information relating to proposed or actual litigation involving you and BU.
- Information relating to IT monitoring and/or access to our information services. We use this information to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees.
- Information derived from monitoring IT acceptable use standards.
- Vehicle registration(s).

The name, professional service or faculty, work email address and telephone number(s) for staff will appear in BU's internal email and staff intranet directory. This information will be used by call handling staff to direct external calls and general enquiries accordingly. If a member of staff has any personal and / or safety concerns

about the release of work-related contact information they should contact HR at hrenquiries@bournemouth.ac.uk. Staff profiles for academic staff, senior staff and staff in roles that involve significant contact with external organisations and or members of the public will normally be available online in accordance with BU's policy on the Disclosure of Information on Employees.

**Special Category and Criminal Convictions Data**
We use the following special category and criminal convictions data to comply with our legal obligations and for equality and diversity monitoring (including equality analyses). We also use it to ensure the health, safety and wellbeing of our employees. The special category and criminal convictions data we collect about you includes:

- Information about criminal convictions and offences.
- Health and wellbeing information either declared by you or obtained from health questionnaire(s), occupational health referrals and reports, sickness absence forms or fit notes i.e. Statement of Fitness for Work from your GP or hospital.
- Where you leave employment and the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision.
- Information required for medical physicians and / or pension providers.
- Accident records if you have an accident at work.
- Details of any DSE assessments, access needs or reasonable adjustments.
- Information you have provided regarding Protected Characteristics as defined by the Equality Act and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes ethnic origin, religion or belief, sexual orientation, sexual identity, disability and may be extended to include other protected characteristics.
- Details of any absences (other than holidays) from work including time on sick leave.
- Trade Union membership for the purpose of the deduction of subscriptions directly from salary or withholding of pay (for strike or action short of strike).

**Personal Tutors and Learner Analytics**
Where staff are fulfilling the role of Personal Tutor there will be records of their engagements with students in this capacity. These are in the form of records created by staff themselves in the BU Personal Tutor note-taking system and data reports generated from those records. This information will be created and managed in accordance with the *Personal Tutor policy (5D)* and associated Faculty and BU guidance. Similarly, for those involved in the Learner Analytics there will be records of student engagement and learning. Further detail on this can be found *here* in the Learner Analytics privacy notice and code of practice.

## 4. Lawful basis for processing your personal data

In summary, the majority of data is processed because it is necessary to perform a contract or to take steps at your request before entering a contract with you or your employer or to comply with a legal obligation, such as employment legislation or HESA requirements.

Some processing is carried in the public interest such as when BU is carrying out staffing reviews, wherever possible this data will be anonymised.

We hold emergency contact details which will be used to protect your legitimate and vital interest in an emergency situation. Further, occasionally we may decide that we need to process certain information about you without relying on your consent: for example, because the processing is necessary to protect your or another person's vital interest, to safeguard the welfare of you or someone else or to comply with our legal obligations. In all cases, we will consider that the scope of data being processed and the way in which we will process it means that our approach is proportionate, and the legitimate interests are not outweighed by damage to the rights of the individuals.

Where required we will obtain your consent to use your personal information, for example to set up a job alert by email.

Some information is processed in order to ensure the security of our network and to protect data in our care.

Specifically, we rely on the following lawful basis for processing your personal data under the UK GDPR:

•performance of a contract or to take steps at your request before entering a contract.
• comply with our legal obligations.
• protect your vital interests or those of another person.
• performance of our public task.
• purposes of our or another person's legitimate interest.

**Criminal convictions and offences**

In relation to criminal convictions and offences, processing of this nature is necessary to meet our legal obligations and will be subject to suitable safeguards.

**Special category data**

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

• explicit consent.
• carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
• protect your vital interests or those of another person where you are incapable of giving your consent.
• personal data manifestly made public by you.
• establishment, exercise or defence of legal claims.
• processing is necessary for reasons of substantial public interest.
• archiving purposes in the public interest or statistical purposes.

In addition we rely on the processing condition at Schedule 1 part 1 paragraph 1 of the Data Protection Act 2018. This relates to the processing of special category data for employment purposes.

## 5. How we hold your personal data and for how long

Much of the personal data described in the rest of this Notice will be held in electronic form in systems provided or hosted by BU, including systems we have procured from third party providers. Separate privacy information will be given to you about some of these systems. Some of your information may be held in cloud-based systems. We enter into agreements with IT service providers so that we have appropriate assurances in place regarding the functionality and security of their systems, to ensure that your data is processed in compliance with the data protection laws which apply in the UK.

Data relating to your job application and our communications with you at the applicant stage is held within a cloud hosted, electronic recruitment system called Eploy. Any applicant data processed prior to our implementation of Eploy, but within the relevant retention period, is held within relevant electronic files which are secured with access permissions.

BU uses a cloud hosted electronic staff record and payroll system called iTrent for employment records. We have skeleton records relating to employment held in archived versions of previous systems called Bond and CoreHR. In addition, BU uses several different platforms for the purpose of development and training. These include KnowBe4, WorkRite and Brightspace.

**More information:**

There is an individual iTrent record for each current and former member of BU staff. This information is held within iTrent during the period of your employment and for six years afterwards. The information held includes information such as your name, title, addresses, telephone numbers, and personal email addresses, qualifications, job title, salary, payslips, your bank details and emergency contact and other key aspects of your employment contract with BU. Six years after employment ceases only the following core meta data will be retained: Name, Date of Birth, NI number, and BU dates of employment.

Electronic employment records about you are accessible to other BU staff to the extent that they require access for the purposes of their role within BU, to fulfil our employment duties with you (such as to process payroll, sickness, annual leave and IT access) and where a legitimate and vital interest exists (such as in an emergency). BU uses MHR UK as a data processor to support the running of the iTrent system.

If you are a BU employee, some types of information which are held securely within iTrent will also be separately held in electronic and/or hard copy by the Faculty or Professional Service in which you work including information about any appraisal and development matters and any additional support needs you may have.

Your personal data will also be held in electronic and/or hard copies within files and email folders in individual BU administration departments as appropriate. This includes information held by our Human Resources (HR), Health, Safety and Wellbeing and Payroll teams, RDS (for the purpose of grant bidding and REF), Estates (Parking Permits) in relation to the services they provide to you and to BU, and your interactions with them. It will also include any information generated through your decision to access additional services provided by or through BU such as the Employee Assistance Programme, Occupational Health, Staff Benefit Schemes, Coaching and development.

**How long we keep your personal data**

We will aim to retain your personal data only as long as necessary for the purposes of the processing which are explained above, and any secondary purposes such as audit, regulatory and legal record-keeping requirements. In general, we apply the following principles to determine how long we will keep your data:

| Record group | **Retention period*** |
|---|---|
| Applicant records including personal details, job applications and interview records | Six (6) months of the date consent was last provided in the online recruitment system, or six (6) months after the outcome of the latest application, whichever is later |
| Employee records (records containing employment data of individual members of staff including Written Particulars of Employment, Contracts of Employment, Changes to Terms and Conditions of Employment, Termination of Employment, details of performance, training and absences unrelated to health surveillance records) | For the duration of employment and up to six (6) years after employment ceases |
| Employee records administration (database records for all current and former employees, including Name/DoB/NI number/BU start and end dates) | For the duration of employment and up to six (6) years after employment ceases after which only the following core meta data will be retained: Name/DoB/NI number/BU start and end dates |
| Records documenting entitlements to, and calculations of, Statutory Payments | For a period of three (3) years following the end of the tax year to which they relate |
| Records documenting health surveillance records including details of absences of an employee relating to health surveillance | For the duration of employment and up to forty (40) years from date of entry after employment ceases dependent upon causation |

These principles may only be departed from where it is necessary and proportionate for BU to keep the record for a longer period. For example, if the record is, or is likely to be required, for evidential purposes; if BU is subject to a legal obligation to retain the record for an additional period, or where the record is required by BU for another lawful purpose (for example, where the basis for our processing changes over time due to developments in circumstances or in our relationship with the individual).

## 6. Data Sharing

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including our data processors, training providers, government agencies (including the Health & Safety Executive, Local Health Authorities/Trusts, etc) and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions, statutory payments (such as maternity, adoption, etc).

This Notice describes planned, regular data sharing and types of one-off data sharing which we know will usually arise. There may be additional one-off circumstances in which we share data with third parties which are not covered in this Notice or other privacy information, such as where a government or other public sector body exercises a legal right to require information in relation to a specific situation. We will only share information with third parties where we are satisfied that the sharing complies with the data protection laws.

We will disclose limited staff data to a variety of recipients including:

- our employees, agencies, BU and subsidiary company Board members and contractors where there is a legitimate reason for their receiving the information (including service providers, such as our external IT support providers, our insurers and external legal and financial advisers)
- current, past or potential employers of our staff (to provide or obtain references with your consent. In line with BU classification guidance, any reference received or provided by BU is treated as confidential
- letting agents, banks, mortgage companies (to provide references with your consent)
- professional and regulatory bodies (e.g. NMC, HCPC, BPS, SRA, BSB, ACCA) in relation to the confirmation of conduct including complaints, job description and information provided as part of the recruitment process
- Companies House in respect of director and company secretarial appointments and resignations for BU subsidiary companies (with your consent and in accordance with our legal obligations)
- external organisations for the purposes of gaining professional accreditations or memberships (e.g. AACSB, AMBA. EQUIS). This information may include your name, career history, membership of professional associations and your publications
- external assessors in respect of recruitment information relating to Professorial or Senior roles
- UK Higher Education Funding Bodies and associated organisations including the REF, Research England, UK Research & Innovation, DfE, HEFCE and HEFCW and SFC
- if your appointment is externally funded, the relevant funding body
- the Higher Education Statistics Agency (HESA) on an annual basis in respect of anonymised data on our staff and Board members. For further information on how HESA collect and process information please see their website: https://www.hesa.ac.uk/about/regulation/data-protection/notices
- government departments and agencies where we have a statutory obligation or other legal basis to provide information (e.g. Her Majesty's Revenue and Customs (HMRC), the Higher Education Funding Council for England (HEFCE), the Home Office (in connection with UK visas and immigration))
- for roles that require security and criminal records checks, you'll be asked to share your data with the Disclosure and Barring Service (DBS) and GBG Group, our external provider of online disclosure services
- third parties who work with us to provide staff support services (e.g. coaching and mentoring and occupational health services)
- third parties who are contracted to provide out–of–hours IT services for us
- other higher education providers or employers where the member of staff is taking part in an exchange programme or other collaboration as part of their employment
- external organisations including funders and third-party clients (for example, where our member of staff is named as part of a research application for external funding or is to be involved in providing consultancy services to an external organisation)
- crime prevention or detection agencies (e.g. the police, security organisations, Department for Works and Pensions and local authorities)
- pension providers (including, TPS, NHS, USS, LGPS)
- emergency contacts (but only where we have consent from the member of staff or there is a legitimate reason for the disclosure)
- healthcare, social and welfare organisations
- representatives of a current, former or potential member of staff (but only where we have consent from the member of staff or there is a legitimate basis for the disclosure)
- internal and external auditors
- debt collection and tracing agencies
- courts and tribunals
- local and central government
- trade union and staff associations (where information is already in the public domain or we have consent from the member of staff)
- survey and research organisations, for example the annual staff survey
- publications press and the media
- to the new employer, where staff transfer to another organisation under TUPE regulations as required by law

- software and data hosting providers, this will be subject to a formal data sharing agreement between BU and the supplier
- internal or external auditors or investigators for the purposes of an internal or external audit or investigation.

Certain personal information about our staff is available in the public domain and is shared on our website. Data that is publicly available world-wide and may be disclosed to third parties, includes;

- Names of members of the Board, Committees and Senate
- Names and academic qualifications of staff
- Staff biographies
- Workplace contact details
- Other information relating to staff that they have agreed to share in the public domain or on our website.

We will send some of the staff information we hold to the Higher Education Statistics Agency (HESA). This does not include the name or contact details of staff. HESA collects and is responsible for the database in which HESA staff records are stored. HESA uses that information in its own right – to publish statistics about staff in higher education, for example. HESA also processes the information held in the databases for other organisations. The data protection laws also apply to HESA.

If a member of staff provides us with information about their disability status, ethnicity, sexual orientation, gender reassignment, parental leave or religion, this will be included in the HESA staff record. This helps to make sure people are being given equal opportunities and to prevent unlawful discrimination. HESA will not use this information in any way to make decisions about you.

For more information about the way HESA use staff information please visit the HESA website which contains the staff collection notice.

**Non-routine data sharing in exceptional circumstances**

We will share personal data with emergency services and/or the person you have identified to us as being your emergency contact, where this is necessary to safeguard your position or that of other individuals.

**More information:** We will also share personal data with the police or other organisations with responsibility for investigating potential crimes such as fraud (e.g. local authority fraud investigation teams) where satisfied that this is necessary for the prevention or detection of crime. This may include sharing special category data such as health information.

Depending on the nature of the situation which has arisen, sharing with the emergency services could include sharing information with the police, National Health Service organisations and the Fire Service. This will be when disclosure is necessary to protect your vital interests, i.e. where you are at clear risk of harm, or to protect the vital interests of others e.g. if they are at risk of harm from your actions. We will only share special category data on this basis if it is not possible for us to obtain a valid consent from you to the disclosure. Where the police have told us, and we are satisfied that this is the case, that sharing your data with them is necessary for the purposes of preventing or detecting crime. Disclosure is necessary for the purposes of protecting you or others from risk of harm, or for prevention/detection of crime: these are purposes in the substantial public interest.

## 7. Overseas transfers of personal data

Data protection laws limit our ability to transfer personal data outside the countries within the UK and countries, such as the those within the European Economic Area, which are subject to an adequacy decision and which are subject to the same or very similar data protection laws (Restricted Transfers). This is to help ensure that a consistent level of data protection applies to your data at all stages of processing, and that you are not exposed to additional privacy risks through the transfer of your data. Restricted Transfers are only permitted in certain circumstances. Where such Restricted Transfers are necessary, we ensure that we have appropriate safeguards in place.

There may be a Restricted Transfer of your personal data in the following circumstances:

- Where we use a cloud-based IT system to hold your data, and the data in the cloud is stored on servers located outside the UK in a country which is not subject to an adequacy decision. In these circumstances we safeguard your data through undertaking appropriate checks on the levels of security offered by the cloud provider and entering into a contract with them which applies protections of the same type and level required by data protection laws within the UK;
- Where you are based outside the UK in a country which is not subject to an adequacy decision and we need to send you emails or other communications which are necessary for the performance of our contract with you or for implementing pre-contractual measures which you have asked us to take (e.g. processing your application or enquiry). In these circumstances the data protection laws say that transfer is permitted; or
- With your consent.

## 8. Your rights as a data subject and how to exercise them

As an individual you have certain rights regarding our processing of your personal data, including a right to lodge a complaint with the Information Commissioner as the relevant supervisory authority.

Under the data protection laws you have a number of rights in relation to our processing of your data. In summary these are:

- Right to request access to your data as processed by BU and information about that processing (a "subject access request")
- Right to rectify any inaccuracies in your data
- Right to request erasure of your data from our systems and files
- Right to place restrictions on our processing of your data
- Right to object to our processing of your data
- Right to data portability: where we are processing data that you have provided to us, on the basis of consent or as necessary for the performance of a contract between us, you have the right to ask us to provide your data in an appropriate format to you or to another controller.

You are entitled to request a copy of the data you provide to us in an electronic format so that you may pass that data to another body (the right to data portability), as well as to request a copy of the data we hold about you (a Subject Access Request).

You are also entitled to raise an objection to the processing where the processing of data we hold about you is likely to cause you damage or distress, and to request either the rectification of any incorrect data, the restriction of any further processing of your data or the erasure of your data (right to be forgotten).
You have the right to withdraw your consent for processing your personal data where we have originally asked for your consent. However, where we collect your personal data under another legal basis, it may not be possible for us to remove all of your personal data from our records if you request this.
Most of these rights are subject to some exceptions or exemptions, depending on the purposes for which data is being processed.

If you have any questions or concerns about our processing of your data, please contact the **BU Data Protection Officer (DPO)**:

Email: dpo@bournemouth.ac.uk
Telephone: 01202 962472
Address: Poole House, Bournemouth University, Fern Barrow, Poole BH12 5BB

If you would like to exercise any of your rights as outlined above, you can contact the DPO as above or visit the Data Protection page on our website to access the relevant forms.

We will always aim to respond clearly and fully to any concerns you have about our processing and requests to exercise the rights set out above. However, as a data subject if you have concerns about our data processing or consider that we have failed to comply with the data protection legislation then you have the right to lodge a complaint with the data protection regulator, the Information Commissioner:

Online reporting: https://ico.org.uk/concerns/
Email: casework@ico.org.uk
Tel: 0303 123 1113
Post:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

**Disclosures in response to information requests**

As a public authority and controller we receive information requests under the Freedom of Information Act 2000 and the UK GDPR and we must consider whether to disclose information about our staff in response to these requests. We will normally disclose work-related information about staff in a public facing role. We may also disclose information about staff members whose work is purely administrative if their names are routinely sent out externally. It is less likely that information about those who do not deal directly with the public in an operational capacity will be disclosed. The Executive Team and the University Leadership Team will have more information disclosed about them, such as photographs and biographical detail, due to their position at BU. We will consider withholding information if we think that it will prejudice our commercial interests or the conduct of public affairs or the rights and safety of our staff, irrespective of grade or position.

The type of information you can expect we will routinely disclose is as follows:

- Name and work contact details.
- Pay bands (not your exact salary).
- How long you have worked at BU, your current role, any previous roles or secondments and what your role involves.
- Your position in the corporate structure.
- Business related entries in your diary/calendar.
- Summaries of expense claims without details of where you stayed, where you ate or your itinerary.
- Any work-related training at BU.
- Any work-related minutes.

The list above does not include every area where we might disclose information about you. The type of information provided will only concern your professional life at BU. We will not disclose non-work related personal or special category data under the Freedom of Information Act 2000.

We will consult with you prior to deciding whether to disclose any information that we consider would not be within your reasonable expectations.

## 9. Further Information

**The Recruitment Process**

BU processes your personal data to take steps at your request before entering a contract with you. We will also process your personal data to enter into a part time hourly paid contract or a permanent employment contract with you if you are appointed.

We will share your personal data internally as needed for the recruitment exercise and any appointment, including with HR members, recruitment panel members, interviewers, the recruiting manager, and payroll.

Occasionally, external individuals may serve as experts on selection panels. In such cases, the University will provide applicant details to these individuals via the candidate management system for recruitment purposes.

Except as set out in this Notice, BU typically does not share your personal data with third parties. However, for pre-employment checks, we will gather references and verify your right to work through an approved identification document validation technology provider. We will share your data with former employers for references, background check providers, and the Disclosure and Barring Service for criminal records checks, where necessary. If an external funding body directly funds your employment, your payroll data and CV may be shared with them.

If your appointment is grant-funded, salary information and your CV may need approval from the external funding body. If your role involves working with third-party organisations such as the NHS, information about your employment may be shared with them.

BU utilises Atlantic Data Ltd, a third-party organization, to administer Disclosure and Barring Service (DBS) checks on our behalf. BU shares limited personal details with Atlantic Data Ltd for this process (such as title, forename, middle name, surname, gender, date of birth, email). A copy of Atlantic Data Ltd.'s privacy statement is available here: https://policydocuments.disclosures.co.uk/Privacy_Statement.pdf

**Campus Facilities**

We process your information in a number of ways in order to manage the BU estate (land and buildings) on the Talbot, Lansdowne and Chapel Gate sites, so that we can provide a safe, secure, efficient and well-managed environment. This includes:

- Operation of CCTV systems. Data generated through the operation of these systems will in certain circumstances be shared with the police.

CCTV systems are in place in some parts of BU's estate for the purposes of ensuring a safe and secure environment, preventing crime and anti-social behaviour and facilitating the detection or prosecution of criminal behaviour. CCTV footage is processed in accordance with BU's CCTV policies and procedures. Access to the footage is securely controlled by BU's IT security arrangements. We may provide CCTV footage to the police where they believe that a crime has been or may have been committed and we are satisfied that the CCTV footage may assist them in their investigation and disclosure would comply with the data protection legislation.

- Management of car parks and provision of parking permits. This includes sharing data with the third party provider of parking enforcement services.

Your data is processed within BU when we process any application you make for a BU parking permits. A third party provider carries out monitoring and enforcement of the terms and conditions of use of BU car parks. Separate privacy information about this processing is provided on the signs in BU car parks and when you make any application for a BU parking permit.

**Trade Union Membership**

The recognised unions at BU (UCU and UNISON) are controllers for the personal information connected to your union membership. BU holds some union subscription details in order to process salary deductions for union membership for which you will have given your consent.

**Monitoring of staff**

All of our IT systems are auditable and can be monitored, though we don't do so routinely. We are committed to respecting individual users' reasonable expectations of privacy concerning the use of our IT systems and equipment. However, we reserve the right to log and monitor such use in line with our Acceptable Use Policy

and BU Staff and Authorised Users Information Security Policy. BU reserves the right to use monitoring activities to protect against threats to its students, staff and to BU itself.

**Smartcard passes**

All staff are all issued with a Smartcard pass that displays their name, staff reference number and photograph. This is a multi-function card and contains key information that is utilised by a number of systems around BU, including for the swipe access system for the entry and exit of our premises . Smartcards details (names, numbers and photographs) are held on BU Servers controlled by Estates and can only be accessed by a restricted number of people. Any data recorded by the Audit Trail Function (Audit Trail Data) will not be used for monitoring individuals, except for the purpose of the prevention and detection of crime or in a life or death situation (see BU's Code of Practice for Access to Smart Card Data for further details).

Should you lose your pass you will need to contact smartcardservices@bournemouth.ac.uk. The Smartcard policy and Smartcard FAQs provide further details.

**Disputes**

BU will use the information it holds as necessary for establishment, exercise or defence of legal claims which are or may be taken against it. For this, your data will be processed by relevant contacts within the Professional Service or Faculty, our internal Legal Services team as well as any external legal advisor and BU's insurer, U.M. Association Limited. BU uses Shakespeare Martineau LLP for external legal support for employment related disputes.

**IT Service Desk Calls**

Calls are recorded for quality and training purposes. The recordings are only used to improve the Service Desk service provision. The call recordings are deleted after 3 months.