PRIVACY NOTICE FOR EMPLOYEES

Introduction

This privacy notice explains how Birmingham City University ('BCU') collects, uses and shares your personal data, and your rights in relation to the personal data we hold.

It applies to all employees, workers and contractors.

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

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services.

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

BCU is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations. This privacy notice explains the following:

1. How we collect your information 1
2. What information does the University collect? 1
3. How we use your personal data 3
4. Who has access to the data and who does BCU share data with? 6
5. How does the organisation protect data? 8
6. How long will BCU keep my data? 8
7. What happens if an employee does not provide personal data? 9
8. Your rights 9
9. How to ask questions or raise concerns 9
10. Changes to this privacy notice 10
11. Where can I get more information? 10

1. How we collect your information

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, or other background check agencies and information from criminal records checks permitted by law.

We will also collect additional personal information in the course of job-related activities throughout the period of you working for us.

2. What information does the University collect?

The University may collect a range of information types about you, including:

- your name, address and contact details, including email address and telephone number, date of birth and gender;

- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependents and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record (if applicable);
- Psychometric/ personality tests and analysis (if applicable);
- Details of working patterns and attendance at work, including employee requests for flexible working;
- Details of all periods of leave taken, including (but not limited to) holiday, sickness absence, unpaid leave and sabbaticals, maternity/paternity/adoption/shared parental leave, dependent leave, compassionate leave, and the reasons for the leave; and return to work forms and assessments
- details of any informal or formal disciplinary, grievance or complaints procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, probation and other performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence.
- Exit interview / exit questionnaire.
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments; Information relating to employees' health and safety at work including for work-based travel.
- details of trade union membership;
- equal opportunities monitoring information, including information about your race, ethnicity, sexual orientation, health and religion or belief.
- Digital footprint data made in the context of the use of computers and other electronic devices used for work purposes including the access of work buildings, work software and systems, internet access, BCU app and CCTV. Further information is available in the IT policies.
- Personal data held in recordings (e.g. lecture capture) of teaching sessions or public seminars/ talks given or attended e.g. visual image, name and any other personal data employees share in these sessions.
- For certain roles, for example, governors, senior management and directors of BCU subsidiary companies, Birmingham City University may need to carry out checks to confirm that the person is 'fit and proper' to be an accountable officer and charity trustee. This involves the processing of personal data.
- Your GPS location if you travel for work or study purposes within scope of BCU insurance and 'check in' to a location via the designated app / website.
- Membership of internal staff networks (for the purposes of facilitating the networks).
- Membership of sector professional networks (where funded by BCU or where you have informed BCU that you are a member of such a network).
- Your participation in BCU related competitions.

The University may collect this information in a variety of ways. For example, data might be collected through application forms, CVs; obtained from passports or other identity documents such as driving licences; forms completed by employees at the start of or during employment; from correspondence with employees; or through interviews, meetings or other assessments.

In some cases, the University may collect personal data about its employees from third

parties, such as recruitment agencies, references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law. Where necessary the University will seek information from third parties with the prior consent of the employee(s) in question.

Data will be stored in a range of different places, including employee personnel files, in the University's HR management systems and in other IT systems (including the University's email system).

3. How we use your personal data

BCU needs to process data to enter into an employment contract with you and to meet our obligations under your employment contract. For example, we need to process your data to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements if applicable.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For specified positions, it may be necessary to carry out criminal records checks to ensure that individuals are permitted to undertake a particular role.

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship.

Processing employee data allows the organisation to;

- operate recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- Operate and keep a record, and where relevant casework, of employee performance and related processes; including but not limited to appraisal, career development, promotion or capability procedures. This includes planning continued professional development, planning for career development, succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain and use occupational health advice, to ensure that the employer complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- Monitor and respond to staff use of the IT network, devices, software, BCU app etc.
- respond to and defend against legal claims;
- maintain and promote equality in the workplace.
- provide references on request for current or former employees; and

- respond to and defend against legal claims.
- fulfil its statutory reporting obligations, for example, the HESA Record.
- produce minutes of meetings for business purposes.
- make audio or video recordings of meetings, events and teaching sessions which employees may attend and participate in. The purposes include: minute taking, sharing the event with those invited but unable to attend, continued professional development, distance learning, making reasonable adjustments for people with disabilities in compliance with the Equality Act 2010, assessment and moderation, marketing and historical archiving. Recording will not be covert unless specially authorised through a policy permitting this action.
- run the university account password reset facility (which sends a reset link to a personal email address stored in the system)
- analyse results of questionnaire data for a variety of purposes. The purpose will be stated when someone is given the option of responding to a questionnaire.
- carry out the core functions of the university including student recruitment, the administration of the student learning journey, learning, teaching and research.
- carry out business and management monitoring, review, planning and forecasting
- carry out individual or team profile analysis;
- facilitate travel for work purposes
- carry out employment law obligations - Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities) for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law or for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards of professional confidentiality. An employee may decide to disclose to the employer that they are a member of a trade union. The employment does not keep a register of this, however if an employee chooses to be accompanied by a trade union representative in a meeting relating to their employment this will be stated in any letters/ minutes of the meeting as factual record of events. Where the University processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is for the purposes of equal opportunities monitoring. Data that the University uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether to provide such data and there are no consequences of failing to do so.
- commission photography / videography on campus or at specific events, such as award ceremonies, careers fairs, celebratory events etc. for use in its internal and external promotional material or university archive material. Staff may appear on the resulting images, and the resulting images may be published. Once you have left employment at Birmingham City University, if you do not want your photo used in publications that have not yet been produced, please contact of the school office of the School you worked in or other business area that you worked in and also the Marketing and Communications department.
- To maintain relevant suppression lists.
- If you provide any personal data related to BCU's business engagement activities, e.g. signing up to an event, BCU may process relevant personal data about you.

Your staff photo will be displayed:

- on your staff ID card and the computer systems related to campus and computer system access
- on communication systems and other online environments (Outlook, Teams, Moodie, Mahara etc.)

- on the staff directory (intranet and for some staff, the website)
- in publications such as, but not limited to, school/ college newsletters, staff newsletters, University news articles and promotional/ marketing publications which may be printed, circulated electronically or accessible on the intranet and internet. If you are at any event where there is photography and you do not wish to be in the photography, please speak to the photography to ensure that you are not close enough in shot to be identifiable.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Relevant staff may also have physical information processed if they are teaching on sport / physiotherapy related courses, where they are using themselves as demonstrators. Information about Trade union membership is processed to allow the organisation to operate check-off for Trades union subscriptions.

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

You have some obligations under your employment contract to provide BCU with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the terms of your employment contract, professional regulatory requirements or under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights. If you do not provide certain information when requested, we may also not be able to perform the employment contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

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

BCU may use artificial intelligence (AI) where it may bring benefits to the university and the university community of students, applicants, enquirers, alumni and staff. Please be assured that BCU will only use AI where it has been assessed as safe and appropriate. BCU makes every effort to ensure that it meets its' legal obligations under data protection laws when using AI tools in order to protect your personal data.

More detail about the data protection legal background of processing personal data relating to staff health and wellbeing

To process personal data at least one lawful basis must be identified under Article 6 of the UK GDPR. A variety of lawful bases may apply depending on the exact situation. The most relevant legal bases would that the processing is necessary for the performance of contract as the university needs to carry out certain tasks to fulfil its responsibilities in the contract relating to the staff member, for the performance of a task carried out in the public interest' to fulfil the core missions of the university, to fulfil legitimate interests of the staff and /or the university and / or a third party, or to fulfil the University's legal obligations, including under

the Equality Act 2010. Staff implementing the policy should contact informationmanagement@bcu.ac.uk if they want advice on which lawful basis applies or assistance on completing a Legitimate Interests Assessment.

Where special category data (such as health data) is processed, a condition of processing must also be identified. The condition for processing will often be UK GDPR Article 9(2)(g) 'for reasons of substantial public interest'. BCU will sometimes rely on the substantial public interest conditions in the Data Protection Act 2018 Schedule 1, Part 2, paragraph 6 'Statutory etc. and government purposes' or paragraph 16 'Support for individuals with a particular disability or medical condition'. BCU will also sometimes rely on UK GDPR Article 9(2)(b) 'Conditions relating to employment, health and research etc.' The most relevant paragraph for this is Data Protection Act 2018 Schedule 1 Part 1 paragraph 1 'Employment, social security and social protection'. There may also be circumstances where UK GDPR Article 9(2)(c) 'vital interests' (to protect a life) applies.

Please note, the lawful basis 'public interest' and the condition of processing 'substantial public interest' do not mean that the information is made publicly available. Instead, they mean that it is in the good of society (i.e. it's in the public good) that organisations can use such information to support people with particular disabilities or medical conditions.

Only where no other lawful basis or condition of processing applies, BCU will ask for the individuals' consent / explicit consent. The above means that, as a default, BCU does not need to and will not ask for consent to process this personal data. However, BCU will still treat it with sensitivity.

4. Who has access to the data and who does BCU share data with?

Employee information may be shared internally to fulfill the purposes of the data processing (see 'How we use your personal data'), including but not limited to members of the HR team, Learning & Development, Health & Safety, Payroll, employee line managers, managers in the business area in which employees work, University Management and specific IT staff. In certain departments, personal phone numbers will be shared within the team in order to facilitate shift rotas or for other similar purposes.

BCU may share your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The organisation may also share your data with third parties in the context of a sale of some or all of its business. In these circumstances BCU will always ensure appropriate controls are in place to ensure your data is safe and is only used if necessary for the allowed purpose, following which it will be permanently deleted on completion of the task.

The University will also share your data, if necessary, with third parties that process data on its behalf or who it has a legal obligation to share with, for example:

- Agency staff
- Assessors
- Auditors
- Business Continuity / Risk and Resilience support services
- Consultants and contractors
- Council for Industry and HE / National Centre for Universities and Businesses (NCUB) – researchers only
- Disclosure and Barring Service and related organisations

- Freedom of Information requests / Environmental Information Regulations (EIR) requests. BCU may receive FOI and EIR requests for third party personal data. BCU has a legal obligation to internally process any personal data it holds when considering requests under these laws. BCU will consider whether external disclosure of this personal data would contravene UK GDPR principle (a) lawfulness, fairness and transparency. Where it would, BCU will apply legal exemptions / exceptions and not disclose the personal data. Where this principle is not contravened the exemptions / exemptions relating to personal data do not apply and personal data is released through these kinds of requests.
- Funding organisations, such as Education and Skills Funding Agency (ESFA)
- Government department(s) covering universities, and the Office for Students (OfS)
- Health and Safety organisations, security organisations and the supplier of safety app(s)
- Insurance companies
- Ofsted
- Placement providers
- Police
- Public Health England, Public Health Birmingham and Birmingham City Council (usually this is anonymous statistics and personal data would only be shared if it was mandated and there was a lawful basis for it);
- Training providers
- Travel agents (to facilitate travel for work purposes)
- UKRI (for example as part of the REF)
- UKVI (in circumstances where any employee requires visa sponsorship)
- Organisations processing visa applications (for example for work based travel)
- for the provision of benefits including the employee benefit scheme and pensions;
- the provision of occupational health services and staff health and wellbeing services;
- for legal assistance;
- for the investigation of grievances, disciplinaries or similar. This may include sharing personal data with external consultants;
- for individual or team profile analysis;
- suppliers of IT systems, provisions and software, the website and intranet including the electronic workflows;
- in connection with its statutory reporting obligations such as to the Higher Education Statistics Agency (HESA) (Use the search term 'collection notices' for information about how HESA may use your personal data)
- other services including but not limited to library system suppliers
- in the course of its day-to-day business needs, for example when working in collaboration with other organisations to fulfil contracts, to enable placements, to facilitate research etc.
- for business and management monitoring, review, planning and forecasting

A specific example of sharing data with external organisations is that BCU shares personal data

with a health cash plan provider (as an non-contractual employment benefit), for staff who are covered in the health cash plan provided by BCU. From June 2026 onwards this is for core staff. BCU relies on the lawful basis of legal obligation for this because this personal data is required to add individuals to the policy in accordance with Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) regulatory requirements and for the purpose of medical underwriting and claims handling. Examples of personal data shared for this purpose are name, date of birth, BCU email address and home address. Please direct any questions about this to BCUrewards@bcu.ac.uk

BCU publishes information about researchers and research on its website, available to the general public. The Research Office can be contacted for more information about this.

We also share your personal data if we believe someone's life is in danger or we believe we are compelled to by law.

Additionally some departments have departmental staff contact lists of personal contact details in order to facilitate easier contact between staff for work-related purposes, e.g. for short-notice shift swaps etc. Staff are informed at local level if this is the case in their department. They should speak with their line manager if they do not want to provide this information or be part of the list. This may or may not be possible depending on the job role and purpose of personal data sharing.

Data is stored in a range of different places, including in your personal file, in the University's HR management systems and in other IT systems (including the organisation's email system).

Your data may be transferred to countries outside the European Economic Area (EEA). Data is transferred outside the EEA on the basis of one of the following:

- Where the transfer is subject to one or more of the "appropriate safeguards" for international transfers prescribed by applicable law (e.g. standard data protection clauses adopted by the European Commission);
- A European Commission decision provides that the country or territory to which the transfer is made ensures an adequate level of protection; or
- There exists another situation where the transfer is permitted under applicable law (e.g. where we have your explicit consent).

5. How does the organisation protect data?

The University takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or wrongly disclosed, and is not accessed except by its employees in the performance of their duties. We are legally obliged to use your information in line with all applicable laws concerning the protection of personal information, including the General Data Protection Regulations. A range of administrative, technical and physical security controls are used to ensure a robust approach to protecting data held on University IT systems this is supported by BCU's Information Security Policy. For more information about how the University protects and manages your personal data a copy of BCU's overarching Data Protection Policy and Appropriate Policy Document is available on the policies page of the BCU website.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

6. How long will BCU keep my data?

Your personal data is retained and securely and permanently destroyed in accordance with

the published BCU Retention Schedule. In summary, information relating to your employment contract is usually retained for the rest of the current year plus six years after your employment contract ends. This includes your personal file held by Human Resources. However, some medical information and / or health and safety records may be kept for longer periods if required by law. Research related information is exempt from the data protection principle of purpose and storage limitation and will be processed in accordance with Article 5(b) and 5(e) of UK GDPR.

7. What happens if an employee does not provide personal data?

Employees have some obligations under their employment contract to provide the University with data. In particular, they are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. They may also have to provide the University with data in order to exercise their statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that employees are unable to exercise their statutory rights.

Certain information, such as contact details, right to work in the UK and payment details, have to be provided to enable the University to enter a contract of employment with an individual employee. If employees do not provide mandatory information, this will hinder the University's ability to administer the rights and obligations arising because of the employment relationship and ultimately could result in the termination of contract.

8. Your rights

You have the right to correct or update your personal data at any time. As a staff member please use ERP or log a ticket on the HR Helpdesk. If you cannot do that, you can contact informationmanagement@bcu.ac.uk. You may have the right to have your data deleted, the right to restrict processing, the right to object and / or the right to data portability and you have the right to know about and challenge automated decision making and profiling. Follow the links to find out whether those rights apply in these circumstances. To do any of those things or if you have followed the links but would like clarification, please email informationmanagement@bcu.ac.uk.

You have the right to request to see the personal data we hold about you. You can submit a Subject Access Request (SAR) in accordance with the Subject Access Requests (SAR) Procedure.

The majority of personal data processing by BCU does not rely on the lawful basis of consent. If BCU is relying on your consent to process your personal data, you will have been asked for your consent at the relevant time. If this is the case, you have the right to withdraw your consent. If the consent relates to electronic marketing, please follow the instructions in the marketing messages received e.g. to unsubscribe. If it relates to the Student Inclusion please contact that team. If it relates to something else, please contact the area of the university that you believe is processing your personal data relying on your consent. If your consent relates to participating in academic research, please contact the researcher as this is not data protection consent. Otherwise please contact informationmanagement@bcu.ac.uk.

9. How to ask questions or raise concerns

If you have read this privacy notice and would like further information, you're welcome to contact our Data Protection Officer by emailing informationmanagement@bcu.ac.uk or by post to: Data Protection Officer, Information Management Team, Legal Services, Birmingham City University, Floor 1, Joseph Priestley Building, 6 Cardigan Street, Birmingham, B4 7BD, or by phoning 0121 202 4597.

If you are not content with how we handle your information, please follow our Data Protection Complaints Procedure. If you have used that procedure and are unsatisfied with the response you have received, you then have the right to complain directly to the Information Commission (IC). You can find out more about this on the IC's complaints website.

10. Changes to this privacy notice

This privacy notice may be updated from time to time so you may wish to check it each time you submit personal information to BCU. The date of the most recent versions will appear on this page (see version control). We encourage you to check our privacy notice from time to time to ensure you understand how your data will be used and to see any minor updates. If material changes are made to the privacy notice, for instance how we would like to use your personal data, we will provide a more prominent notice (including, for certain services, email notification or correspondence of privacy notice changes).

11. Where can I get more information?

Birmingham City University's Data Protection Policy and Appropriate Policy Document

Birmingham City University's Privacy Notices

The Information Commission (IC) information for members of the public

Version: 20
Updated: 27/10/2026