

Staff Data Privacy Notice

This Privacy Notice explains how we, University College Birmingham (the “**University**”) of Summer Row, Birmingham, B3 1JB, telephone number: 0121 604 1000, use the personal data we collect. The University collects personal data from you when you apply for or start employment. We will also update information during your time at the University, such as Professional Development Records (PDR), attendance, payment history etc. We are the data controller for such personal data relating to you and this Privacy Notice explains how we will process your personal data.

Staff personal data is held on the University’s main HR System and various in-house databases and some data is held in paper form. All of the information we hold is held securely and only authorised staff can access it. The information that we collect will be held in accordance with the General Data Protection Regulation 2016/679 (the “**GDPR**”) and the Data Protection Act 2018.

The University’s Data Protection Officer is the Head of Information Services:

Ruth Cartwright

Address: University College Birmingham, Summer Row, Birmingham B3 1JB

Email: dataprotection@ucb.ac.uk

Telephone: 0121 604 1000

There are certain principles that the University must adhere to. This means that we will make sure your information:

- Is treated fairly and is only used for the purposes for which we have collected it and for which we have a legal basis for processing.
- Will only be used for the purposes for which it was collected, unless we ask your permission to use it for something else.
- Will not be excessive. i.e. We will not hold information about you that we do not need.
- Will be accurate.
- Will not be kept longer than is necessary.
- Will be kept securely so that there is no loss of data or data breaches. Personal data is kept on secure servers and any hard copies are kept in secure locations. Only authorised people have access to your personal information. We will ensure that, where personal data is shared and stored outside of the European Union, there are appropriate safeguards in place to protect your personal data.

You have certain rights as a data subject under the GDPR. This means that you have:

- The right to gain access to your personal data – You can ask us what information we hold on you.
- The right to rectification – You can ask us to put right any information that you believe is incorrect or where appropriate, given the purposes for which your data is processed, the right to have incomplete data completed.
- The right to erasure – You can ask for information to be removed, although this is a limited right which applies, among other circumstances, when the data is no longer required or the processing has no legal justification. There are also exceptions to this right, such as when the processing is required by law or in the public interest.
- The right to restrict processing – If you feel you are being disadvantaged by us holding information that is inaccurate, you can ask us to stop processing it until we fix it, or come to an agreement.
- The right to data portability – You can ask us to extract your information so that you can use it elsewhere.
- The right to object – You can object to us processing your data for marketing purposes. You can also object to us processing your data when such processing is based on the public interest or other legitimate interests, unless we have compelling legitimate grounds to continue with the processing.
- Where the legal basis for processing your personal data is based on your consent, the right to withdraw your consent at any time.
- Rights in relation to automated decision making and profiling – However, the University will never make any decisions about you without any human intervention.

For any information on your rights, or if you have questions or concerns, please contact the DPO.

You also have the right to complain to the Information Commissioner's Office (ICO) if you feel that the University is not processing data correctly. You can make a complaint on the ICO's website: <https://ico.org.uk/> .

Why does the University need information about you and what is the purpose of our processing?

We only process data for specified purposes and if it is justified in accordance with data-protection law. Personal information about you will be held by the HR department. It will be used for the following purposes:

- To hold a record of staff employed at UCB
- To make salary payments
- To monitor equal opportunities
- To accurately liaise with the Teachers' Pensions and the LGPS Administrator
- To contact you should the need arise

- To contact your next of kin/emergency contact in the event of an accident/emergency at work
- To monitor professional development
- To monitor attendance and absence
- To enrol with Private Health Insurance provider
- To monitor salary sacrifice schemes
- To meet our obligations in respect to Government returns

What personal data do we hold?

Information that the University holds could include the following:

Biographical Information

Name, job title, gender, ethnic origin, nationality, disability, date of birth

ID card image – This is held for identification, access control and security purposes.

Contact Details:

Home address, contact details, next of kin

Employment Information

Job title, payroll number, pension details, salary grade, salary point and salary, contract details, date employed, date of current role, role descriptor, disciplinary information, probation reports, medical reports, fitness to travel overseas, health information, previous employment history, academic history, absence record, professional development reviews and records, salary payment history, terms of employment, teaching observations, immigration status, details of any parental/maternity/adoption leave, reason for leaving (if applicable), professional affiliation/membership of professional organisations, salary sacrifice schemes, CVs

Information on criminal convictions

Staff usage of UCB systems may be analysed to monitor usage so that UCB can ensure that systems are being used effectively to support students.

CCTV

CCTV is used within the University for security reasons and your image may be recorded.

How long will we hold your data?

All current staff have a personal file. We will retain staff personal file for the duration of your employment and for a period of 6 years following the end of your employment. Pension information may be held indefinitely or until there is no longer a legal basis for holding it. Personal information held on HR systems remains on file in order to provide requested references etc. in the future. After 6 years, your personal information can be deleted at your request.

CCTV data will be deleted after 31 days.

Library – Library records are deleted annually unless there are outstanding issues such as overdue books or outstanding fines.

Who might we share your information with?

On occasion we may need to share your data internally and with third parties. The following is a list of organisations with which we may share information. It is not an exhaustive list, but any organisation with which we share information will have confirmed their compliance with the GDPR.

- Our HR administrators
- Statutory Government bodies
- Birmingham City Council Payroll and Pensions Service
- Teachers' Pensions
- Private Healthcare Provider
- Local Government Pension Scheme
- Local Authorities
- Independent Medical Advisor
- Internal and external auditors
- Employers/sponsors
- Placement providers
- Franchise organisations
- Canvas
- Counter Solutions (Way2Pay EPOS System)
- Library Online resource providers
- Software providers that the University use may need access to resolve IT issues
- Paper Escape Document Scanning (Scanning staff files only)
- Box (Cloud storage of staff digital files)
- Relevant authorities dealing with emergency situations at the University*
- Any other authorised third party to whom the University has a legal/contractual obligation to share personal data with

*Please note that in emergency situations where the University deems it to be in your (or potentially a third party's) 'vital interests' the University may share your personal data, including sensitive personal data with relevant individuals/agencies, e.g. the Police.

****Declaration by the Higher Education Statistics Agency**

The Higher Education Statistics Agency (HESA) collects student and staff information on behalf of the Higher Education Funding Council. The data is processed in accordance with the Data Protection Act and further information about how the data is collected and used can be found at:

<https://www.hesa.ac.uk/about/regulation/data-protection/notices>

Legal basis

The legal basis under which the University processes the above information is as follows:

Processing is necessary for the performance of a contract (See GDPR Article 6(1)(b)) or to take steps to enter into a contract and we will be unable to employ or pay you without processing your personal data.

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller (see GDPR Article 6(1)(e)) and for statistical and research purposes (see GDPR Article 89).

Processing of health-related data is necessary so that we can meet our obligations in the field of employment law (see GDPR Article 9(2)(b)).

Processing of criminal offence information is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (See GDPR Article 9(2)(g))

<i>Version Number</i>	<i>Date Last revised</i>	<i>Revised By</i>
1.0	01/05/2018	DPO
1.1	12/03/2019	DPO
1.2	27/04/2020	DPO
1.3	09/06/2021	DPO/CH
1.4	05/11/2021	DPO