Student Admissions Applications 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 here to study a course. We are the data controller for such personal data relating to you and this Privacy Notice explains how we will process your personal data.

Personal data is held on various systems within the University or in the cloud and, in some cases, 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. You can help us with this by making sure your details are correct by emailing admissions@ucb.ac.uk with any updates to your information.
- Will not be kept longer than is necessary, although some of the data will be archived so that we can still confirm your course, attendance and achievement in the future.
- 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 or stored outside of the European Union, there are appropriate safeguards in place to protect your personal data. Any third party organisations that hold personal data (e.g. cloud hosting, agents) will have confirmed their compliance with GDPR before data is processed.

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. Specifically:

- We need to know who you are, so we will need to check official ID to make sure our information is accurate. Our information must be accurate so that any certificates we produce are correct.
- We need to assess your eligibility for the course that you have chosen to do, so we need information about your previous qualifications and education

- We need to assess if you have any tuition fees to pay and this is based on information such as age, previous qualifications and where you live.
- We need to be able to contact you about your course, so we need up-to-date contact information
- UCAS have an obligation to monitor equal opportunities and diversity, so we will receive some information that is considered "Special Categories of Data" such as ethnic origin, sexual orientation, religion or gender reassignment from UCAS. We will take special care of this and make no decisions about you based upon it. You have the right to refuse to answer these questions when asked and we can state that you have chosen not to answer.
- We may wish to assess whether you need some extra support with your course. For example, you may have a medical condition that we need to be aware of, or you may have specific learning needs that we can support you with.
- Your information may be used to assist in finance and welfare activities
- We need to ensure we comply with Health and Safety guidance
- We need to make sure the University is kept secure, so you will have an ID created from the information that you give us and your access to the University will be recorded
- We may need to respond to Police requests/checks
- Some data will be used in analytical reports
- In order to seek confirmation and validation of your grades we may contact your previous place of study or the awarding body who provided your certificates and seek confirmation and validation of your grades and certificate authentication.

What personal data do we hold?

Examples of the data that we collect from your through our application systems are as follows;

UCB Direct Application

Student ID number, name, address, email, phone numbers, date of birth, ethnic origin, country of permanent residence, nationality, health and wellbeing information, convictions, course applying for and relevant course details, application information such as year and month of entry, letters relating to your application, decisions made, fees information, Agentdetails, whether you have previously attended the University.

UCAS Application

ID numbers, Unique learner number, title, name, date of birth, gender, application information such as course applying for, decisions, replies, conditions, month and year of entry, address, email, phone numbers, previous school information, country of birth, nationality, care leaver information, disability, special needs, convictions

UCAS Teacher Training Application

ID numbers, Unique learner number, title, name, date of birth, gender, application information such as course applying for, decisions, replies, conditions, month and year of entry, address, email, phone

numbers, previous school information, country of birth, nationality, care leaver information, disability, special needs, convictions

UCB College Application

Student ID number, Name, date of birth, address, parent name & contact details, additional learning needs, criminal convictions, health and wellbeing information, Course information, Offer made,

UCB Clearing Application

Student Id, Name, title, forenames, surname, email address, mobile number, postcode, Course information such as year and month of entry, Course, whether accommodation is required, Student Finance application

Application Information and Entry Qualifications

Information on the qualifications you had when you applied to the University. This may include the awarding body, the date achieved, the subject, the level, the grade. Previous degree information for trainee teachers. Personal statements made through UCAS, or on your application form, offers made, interview invitations, your decision whether to accept the place and copies of certificates/transcripts.

Non-EU Student information

In order to comply with Border Agency regulations, we hold the following for non-EU students:

Country of Birth, Place of Birth, Passport Number, Passport Issue Date, Passport expiry date, place of issue, ID card number, Visa information, Work permit Type, Visa Number, Visa Expiry Date.

Our International Office is required to share this information with the UK Border Agency and to inform them of any withdrawals or lapses in attendance.

UCB Proficiency Test

For students who take the UCB proficiency test, the University will be required to collect biometric data. This will include photographic identification (for example an ID card or a passport) and a video recording of the speaking test. The video recording will be stored in digital format for up to five years. A hard copy of your test paper, along with a digital record of your name and test results will also be stored for up to five years. This information is retained for Home Office inspection purposes.

CCTV

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

How long will we hold your data?

Information held on applicants who are unsuccessful or decide not to attend the University will be deleted from our systems after 3 years. Hard copies of information about applicants who are unsuccessful or decide not to attend the University will be destroyed after 1 year.

If you become a student at the University, information that is held on our student records system will be kept for at least 7 years for audit purposes. Hard copies of student information will be destroyed after 7 years.

CCTV data will be deleted after 31 days.

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 administrative/ IT staff associated with student recruitment activities
- Academic staff in order for them to aid in the decision making process and also to support you once you have started at the University.
- Awarding bodies
- Student Loans Company
- Local Authorities
- College Medical Advisor (Where adaptions are required for special needs requirements)
- Franchise organisations
- Parents/Guardians/Next of Kin (under 19 only)
- University and Colleges Admissions Service (UCAS)
- NCTL (Teacher training only)
- Data Harvesting/Amazon Web Services (Cloud Hosting only)
- UK Border Agency (International non-EU students only)
- Software providers that the University use may need access to resolve IT issues.
- Relevant authorities dealing with emergency situations at the University*
- Aspire – John Smith's (Kickstart Scheme) (where applicable)
- 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.

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 enrol you as a student without 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 will only be done with your explicit consent (see GDPR Article 9(2)(a)).

Processing of data for the purposes of monitoring equal opportunities and checking criminal convictions is necessary for reasons of substantial public interest (see GDPR Article 9(2)(g)), specifically for assessing fitness to study and practise and risk to safety of all individuals at the University.

Version Number	*Date Last revised*	*Revised By*
1.0	*13/04/2018*	*DPO*
1.1	*24/05/2018*	*DPO*
1.2	*10/04/2019*	*RC*
1.3	*05/15/2019*	*RC*
1.4	*04/05/2020*	*DPO*