

## 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.

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 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 UK General Data Protection Regulation (the “**UK GDPR**”), the Data Protection Act 2018 (the “**DPA**”) and related legislation (collectively “**Data Protection Law**”). 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](mailto: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](mailto: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) will have confirmed their compliance with Data Protection Law before data is processed.
- 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 Data Protection Law. 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 you 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 applied for and relevant course details such as month and year of entry, letters relating to your application, decisions made, fees information, agent details, whether you have previously attended the University.

### **UCAS Application**

ID numbers, unique learner number, title, name, date of birth, gender, course applied for and relevant course details such as month and year of entry, decisions, replies, conditions, 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 applied for and relevant course details, offer made.

### **UCB Clearing Application**

Student ID number, name, title, forenames, surname, email address, mobile number, postcode, course applied for and relevant course details such as month and year of entry, 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.

### **International Student information**

In order to comply with UK Visa and Immigration Department (UKVI) regulations, we hold the following for international 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 UKVI 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 4 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 adaptations are required for special needs requirements)
- Franchise organisations
- Parents/Guardians/Next of Kin (under 19 only)
- University and Colleges Admissions Service (UCAS)
- Selected Agencies who assist UCB in the application process
- Department for Education (DfE)
- Data Harvesting/Amazon Web Services (Cloud Hosting only)
- UK Border Agency (International students only)
- Third party providers of credibility interviews (international students only)
- Canvas (Virtual Learning Environment; UCBCONnect)
- 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.

## Third Party Processing

The University may contract selected third-party service providers to process your personal data. These service providers are authorised to use your personal data only as necessary to provide the requested services to us. Unless described in this Privacy Policy, the University does not share, sell,

rent, or trade any data with third parties for their promotional purposes. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit. The following is a list of purposes for which your personal data may be processed by third parties and the service providers by whom it may be processed on behalf of the University.

- Student CRM (Data Harvesting) – UCB use third-party data management providers for the purposes of storing personal data about you and your marketing preferences. Personal data may also be processed to support and improve the services that are offered.
- Email: UCB use third-party email providers for the purposes of sending emails relevant to your interests and application status. Personal data may also be processed for the purposes of personalising emails with your application details and other relevant information. Personal data may also be processed to track your behaviour relating to emails received, including whether you opened the email, and/or clicked any links. Service providers that may process personal data for the purposes of sending emails include: Student CRM, Dotmailer
- Events – UCB use third-party event management software for the purposes of managing bookings for events such as Open Days, Applicant Days and Campus Tours. Personal data will be processed and stored by these providers for making the booking, tracking attendance at events and sending event-based updates. Service providers that may process and store personal data for the purposes of event management include: Student CRM, Eventbrite
- Digital Asset Management: UCB use third-party digital asset management software for the purposes of storing images and videos. With your permission, these images may be used by us for the purposes of marketing and advertising. The service provider that may process personal data for the purposes of image processing is Canto.
- Market Research: UCB use a third-party survey software provider for the purposes of conducting market research. Personal data may be processed by this provider for the purposes of analysing feedback. The survey software provider that may process personal data for the purposes of market research is Survey Planet.
- Online Advertising: UCB use several advertising platforms to inform you about courses, events, news and other information that may be of interest to you. These providers may process personal data to better target our advertisements to you or other potential students. Personal data may also be processed to inform the University about the performance of advertising campaigns. Service providers that may process personal data for the purposes of advertising include: Bing, Google, IDP Connect, LinkedIn, Meta, Snap Inc, TikTok, UCAS, The Student Room, UniCompare, Twitter.
- Online Messaging Platforms: UCB use third-party service providers to enable prospective students and applicants to chat online to existing students and staff of the University. Personal data may be processed by these providers for the purposes of enabling these conversations to take place on these platforms, enabling the University to monitor and track these conversations, and also keep you updated on the University. The service provider that may process personal data for the purposes of online messaging services is Unibuddy; Click4Assistance
- Postal: UCB use third-party service providers for the purposes of sending postal communications. Personal data may be processed by these providers to send postal

communications such as prospectuses, letters, postcards and other materials to you on behalf of the University. Service providers that may process personal data for the purposes of sending postal communications include: Data Bubble, Mailchimp, InLine Marketing.

- SMS/Text Messages: UCB use third-party service providers for the purposes of sending SMS/text messages. Personal data may be processed by these providers for the purposes of sending SMS/text message invitations to events or updates on applications on behalf of the University. Service providers that may process personal data for the purposes of SMS/text messages include: Click4Assistance, JanetText, Student CRM, PageOne
- Social Media/News Monitoring: MRA use third-party service providers for the purposes of sending, monitoring, and responding to social media messages. Personal data may be processed by these providers to collect, store and transmit messages to you that are posted either publicly on social media networks, or privately to the University by direct message. These providers may also monitor the wider internet, such as news websites, blogs and forums for mentions of University Customers for the purposes of news sourcing, alumni relations and reputation management. Service providers that may process personal data for the purposes of social media/news monitoring include: Orlo, Story Comms
- Cookies – Cookies are small pieces of information that a website can store on your computer in order for it to remember something about you at a later time. The information is in the form of a text file, which will only be understood by the web site that initially set the cookie. To find out more, see our Cookie Policy.

## 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 UK 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 UK GDPR Article 6(1)(e))

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 UK GDPR Article 9(2)(g) and Article 10)

<i>Version Number</i>	<i>Date Last revised</i>	<i>Revised By</i>
1.0	13/04/2018	DPO
1.1	24/05/2018	DPO
1.2	10/04/2019	RC

<i>1.3</i>	<i>05/15/2019</i>	<i>RC</i>
<i>1.4</i>	<i>04/05/2020</i>	<i>DPO</i>
<i>1.5</i>	<i>20/01/2021</i>	<i>DPO</i>
<i>1.6</i>	<i>10/06/2021</i>	<i>DPO/EP</i>
<i>1.7</i>	<i>07/09/2022</i>	<i>DPO/AA</i>
<i>1.8</i>	<i>14/03/2023</i>	<i>DPO</i>
<i>1.9</i>	<i>24/01/2024</i>	<i>DPO/AA/CS</i>