UNIVERSITY COLLEGE BIRMINGHAM

DATA PROTECTION POLICY OVERVIEW

This document should be read in conjunction with UCB's full Data Protection Policy and all relevant privacy notices.

1. University College Birmingham (the "University") obtains, uses, stores and otherwise processes personal data relating to potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, suppliers, customers, website users and other contacts. It is our policy to take all necessary steps to ensure that all personal data held by the University is processed fairly and lawfully.

2. The University will ensure that all relevant statutory requirements are complied with and that internal procedures are monitored periodically to ensure compliance.

3. The University will implement and comply with the principles set out in the General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (DPA) (collectively "Data Protection Law") which promote good conduct in relation to processing personal information.

   Article 5 of the GDPR requires that you should be guided by the specific principles when you process personal data. Those principles require personal data to be:

   (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
   (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

   Article 5(2) requires that;
   "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

As the “controller”, the University is responsible for, and must be able to demonstrate compliance with, the principles listed above.

4. The attention of all staff is drawn to the data protection rules and procedures set out by the University in its Data Protection Policy. Staff have a duty to follow these rules and procedures and to co-operate with the University to ensure this policy is effective. Disciplinary action may be taken against any member of staff who fails to comply with these rules and procedures. Please also be aware that the University has multiple privacy notices relating to students, staff, applicants, alumni, visitors etc. and that these should be checked when handling personal data. All security policies and privacy notices are available on the website.
5. The University has a responsibility to ensure that personal data dealt with in the course of its business is handled in accordance with statutory requirements and reasonable steps will be taken by all concerned to ensure this duty is observed.
6. The University will consult with staff periodically to ascertain what measures should be taken to increase awareness of data protection issues and to ensure that all necessary measures are taken to make this policy effective.
7. The University will take such measures as may be necessary to ensure the proper training, supervision and instruction of all relevant staff in matters pertaining to data protection and to provide any necessary information.
8. The University will monitor on an ongoing basis compliance with the provisions of the Data Protection Law by third party processors of the University’s data.
9. The person having overall responsibility for data protection will be the Data Protection Officer (“DPO”), The University’s DPO is Ruth Cartwright, Head of Information Services, 0121 604 1000 extension 2348, dataprotection@ucb.ac.uk. A team of colleagues will have local responsibility for specific areas, and this can be found in the list of Data Protection Champions at https://www.ucb.ac.uk/about-us/data-protection-resources.aspx
10. Each member of staff will have immediate responsibility for data protection matters in his/her own area of work. Any queries should be raised with the relevant officer in 9 above.
11. The Information Technology Development Committee has been charged with periodically reviewing data security arrangements, monitoring the risk of exposure to major threats to data security, reviewing and monitoring security incidents, and establishing and implementing initiatives to enhance data security.

Date last reviewed: 07/09/2022 V 1.3