UCAT DATA PRIVACY POLICY 2026

The UCAT Consortium has official policies which guide its work in specific areas. Each policy is reviewed on an annual basis and any updates reflected in operational processes, website information and other communications to candidates. Where appropriate, policies are made available on the UCAT website.

UCAT policies are underpinned by its commitment to equality, diversity and inclusion (EDI). Any substantial amendments to policies are considered in the light of their impact on EDI.

Contents

1. Introduction

1.1. This policy applies to data collected by The UCAT Consortium relating to potential or actual UCAT test candidates. References in this Privacy Policy to “we”, “us”, “UCAT Consortium” and “The Consortium” are to The UK CAT Consortium (company number 05620264), registered office UCAT, B Floor, Medical School, University of Nottingham, Nottingham NG7 2UH.

1.2. The Consortium is a charity and private limited company which provides an admission test (the “UCAT test”) used by UK and other partner universities (“Consortium Universities”) as part of selection processes for healthcare programmes. The organisation is managed by a Board elected from representatives of the UK universities which are members of The Consortium.

1.3. Pearson Professional Assessments (PPA) deliver and develop the UCAT test on behalf of The Consortium. References to PPA in this document include both PPA and its subcontractors.

1.4. The UCAT test is delivered on computer (at PPA test centres in the UK and worldwide) and may also be Online Proctored.

1.5. Candidates are those individuals who create an account for the purposes of taking the UCAT test. Some candidates will choose not to go on to take the UCAT test.

1.6. The Consortium is registered as a data controller with the UK Information Commissioner's Office for the purposes of the Data Protection Act. The Consortium is committed to ensuring that personal data are handled in accordance with the Act.

1.7. Under Data Protection Legislation, The Consortium is the data controller of data collected by PPA on behalf of The Consortium. In line with the requirements of the DPA The Consortium has a written agreement with PPA (Agreement for the Supply of Test Delivery and Development Services) which outlines PPA's responsibilities in collecting, holding and transferring data on The Consortium's behalf.

1.8. This policy provides information regarding data The Consortium holds in relation to candidates, where those data come from and how they are used in accordance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

1.9. When registering to take the UCAT test, candidates are referred to both the PPA Privacy Policy and The Consortium Data Privacy Policy.

1.10. The Consortium retains personal data for the length of time required for the specific purpose or purposes it was collected, which are set out in this privacy notice. The Consortium may keep data that has been anonymised for longer than this period to allow The Consortium to carry out its research objectives.

2. Information from Children

2.1. The Consortium recognizes the importance of protecting privacy where children are involved. It is committed to protecting children's privacy and complies fully with relevant codes and regulations.

2.2. Candidates who are under 18 are encouraged to read this Privacy Policy with their parent(s) or legal guardian(s) and ask questions about things they do not understand.

3. Why does The Consortium need candidate data?

3.1. Where The Consortium processes personal data on the basis of its legitimate interests (or those of a third party), those interests are to:

- carry out the administration of UCAT tests;
- study how candidates use The Consortium's services to inform communications and business strategies;
- understand the effectiveness of The Consortium's research; and
- defend against or exercise legal claims, investigate complaints and respond to queries.

3.2. The Consortium needs to use candidate data to:

- administer UCAT tests (including data required to book a UCAT test, to verify candidate details and to communicate UCAT test results to Consortium Universities);
- consider candidate eligibility for access arrangements, bursaries and to sit the online proctored test;
- respond to general candidate queries;
- investigate complaints or incidents have that occurred during testing;
- investigate allegations of misconduct;
- undertake internal analysis of how the UCAT tests work including looking at the reliability and differences in performance of particular subgroups;
- undertake and support research aimed at improving the UCAT tests; and
- undertake and support research more broadly related to selection to medicine and dentistry that relates to the core objectives of The Consortium.

4. What data does The Consortium collect?

4.1. At **registration**, PPA collects personal data on The Consortium's behalf. These data are used for The Consortium's legitimate interests in supporting the administration of the UCAT tests and to undertake internal analysis and research studies.

4.2. Data collected includes emails, phone numbers and mobile phone numbers. These may be used to contact candidates in relation to the administration of the UCAT test, reminders and advice regarding the UCAT test and delivery of UCAT test results. These data are never used for broader marketing purposes.

4.3. Data may also be obtained from candidates as part of administrative processes including when they apply for access arrangements/accommodations, apply for a bursary, apply to take the test online, request that their 'fitness to test' be reviewed, submit an investigation request or appeal against decisions made by The Consortium. In general, specific data relating to these processes is retained for the duration of the relevant admissions cycle (usually September the following year).

4.4. '**Special category data'** (as defined by the Information Commissioner) collected by The Consortium includes ethnicity data collected at registration. These data are used to ensure that the UCAT test does not discriminate against or in favour of those from particular ethnic origins. In addition, information about any disabilities candidates may have is also collected at registration in order that The Consortium can be confident that candidates are accessing the support they need when taking the UCAT test. Special categories of personal data may also be collected if candidates make an application for a bursary or access arrangements. How these data are used is described below. If used in research and analysis, such data are fully anonymised.

4.5. Candidates provide personal data to The Consortium relating to a range of administrative processes. This includes Bursary applications, applications for Access Arrangements/accommodations, when making complaints and during other interactions with the UCAT Consortium Office and PPA Customer Services. As part of these administrative processes, the candidate may provide additional evidence which contains their personal data and/or that of third parties. Such personal data is used by The Consortium to support the administrative process. During such processes, The Consortium may need to communicate details to PPA for PPA to provide further details regarding a case or for them to assist a candidate in taking the test.

4.6. Any data received in relation to **access arrangements** and **bursary applications** are retained for the duration of the relevant admissions cycle (usually until September the following year).

4.6.1. The Consortium does not share information regarding access arrangements/accommodations with Consortium Universities without candidate agreement.

4.6.2. If candidates are awarded a bursary and use this to pay for a test, this is flagged to their chosen Consortium Universities when UCAT test results are delivered to them. For clarity, Consortium Universities are informed which of their applicants have been awarded a bursary but do not have access to any other data provided in bursary applications.

4.7. On occasion, The Consortium may **survey** candidates to obtain information to enhance the candidate experience and/or contribute to research projects. For research purposes, The Consortium may link survey data to UCAT test and candidate data. The informed consent of candidates to take part in any survey will be obtained. Candidates have the option to not take part. Researchers using survey data only have access to anonymised datasets as outlined below.

4.8. In the provision of **customer service** and for the performance of the contract, The Consortium and PPA may share candidate information with each other to effectively deal and respond to issues candidates may encounter in the administration of the UCAT test. Personal data processed is pursuant to a contract between them and PPA or in the legitimate interests of The Consortium and PPA. PPA retains these data in accordance with their privacy policy.

4.9. When **attending a test centre** to undertake the exam, PPA collects a photo image of each candidate, their signature and CCTV images for the purposes of safety, security and fraud prevention. Candidates are asked to present a government issued ID with photo and signature and this information is used to confirm their identity. This is necessary for the performance of the contract between the candidate and PPA and is subject to PPA's retention period. The Consortium may require PPA to share this information where investigation is required.

4.10. Please refer to the PPA's separate privacy policy to understand how they use candidate information by clicking here.

4.11. Applicants who are applying to universities in both **Australia/New Zealand** and the UK (including partner universities) are required to take the UCAT ANZ test. Where a UCAT ANZ candidate applies or indicates their intention to apply to UK universities, their UCAT ANZ test scores will be provided by the UCAT ANZ Office to The Consortium.

5. Use of Artificial Intelligence

5.1. We may use artificial intelligence systems to support our processes to consider candidate applications for access arrangements, bursaries and to sit the online proctored test; and to provide responses to candidate

queries. These systems operate within a closed-loop environment, ensuring data always remain under our control.

5.2. Artificial Intelligence tools are used to assist with:
  5.2.1. initial screening of applications against eligibility criteria;
  5.2.2. identifying patterns or indicators relevant to these processes;
  5.2.3. supporting consistency and efficiency in evaluation processes;
  5.2.4. flagging incomplete or inconsistent submissions; and
  5.2.5. providing candidates with general advice in a timely manner.

5.3. Artificial Intelligence systems do not make automated decisions with legal or significant effects. All decisions are subject to meaningful human review and oversight.

5.4. Our Artificial Intelligence systems operate within a closed-loop system, which means:
  5.4.1. personal data are not shared with external AI models for training purposes;
  5.4.2. data are not used to train or improve public or third-party AI systems; and
  5.4.3. processing is restricted to approved systems and authorised personnel.

6. What data does The Consortium share with Consortium Universities?

6.1. The Consortium shares candidate data with
  6.1.1. any UK Consortium Universities candidates apply to through UCAS or other entry routes; and
  6.1.2. other partner Universities (who are Associate members of the Consortium) which candidates apply to or indicate they intend to apply to (when creating their UCAT account).

6.2. PPA on behalf of The Consortium has an agreement with UCAS to share candidate data to support the delivery of UCAT test results to Consortium Universities. PPA provides UCAS with candidate data. This is then used by UCAS to match candidates to any application made to a relevant course at a Consortium University requiring applicants to take the UCAT test ("UCAS choices"). UCAS provides PPA with candidate UCAS choices. The Consortium is then able to provide each Consortium University with a set of UCAT test results for their applicants. If a university has received an application from a candidate and the university has not received that candidate's UCAT test result, the university may access the candidate's UCAT test result from a database using the candidate's UCAT ID. For clarity, as part of this agreement, Consortium Universities cannot identify which other universities their applicants have applied to.

6.3. The data passed to Consortium Universities are UCAT test result data (including personal identifiers).

6.4. If a candidate has been awarded a bursary and uses it to pay for a test, this is flagged to their chosen Consortium Universities when UCAT test results are delivered.

6.5. On occasion a candidate may experience an incident during testing (or have mitigating circumstances) which are investigated and deemed significant enough to result in an annotation. This means that (with the candidate's permission) a short factual statement describing the incident or mitigating circumstances is shared with their chose Consortium Universities.

6.6. The Consortium does not share information regarding access arrangements/accommodations with Consortium Universities without candidate agreement.

6.7. In the event of any candidate being found guilty of misconduct, the outcomes of any investigation may be shared with Consortium Universities or other legitimate third parties such as UCAS. The UCAT Misconduct Policy can be found here.

7. What additional data is required from candidates taking the Online-Proctored UCAT test?

7.1. Candidates who take the online-proctored UCAT test will be asked to agree to the terms set out in PPA's Privacy and Cookies Policy to support their testing experience.

7.2. During an automated check-in process, candidates upload a photo of themselves and share their identification documents ("IDs") on camera. Images of IDs are used for the purpose of ID validation using ID authentication protocols. ID authentication protocols are used in conjunction with biometric facial comparison technology to authenticate identity. PPA may use facial comparison technology for the purpose of verifying identity during the testing session, by comparing facial images to that presented on ID and to facial images captured during the

testing session. PPA, for internal use only, may use images of IDs for the purpose of further developing, upgrading, and improving applications and systems.

7.3. Candidates will be asked to acknowledge and agree to video and audio recording of their entire testing session and to the processing of such personal information and UCAT test data by PPA on behalf of The Consortium. Video and audio recording are used for purposes of identity verification, remote observation, incident resolution, such as fraud prevention, security, and for the integrity of the UCAT test and the testing process.

7.4. If candidates sit an online-proctored UCAT test they will be monitored during their testing session in real time; their face, voice, and workspace are captured and recorded for the purposes of test quality, security, and the integrity of the testing process. Inappropriate or wrongful conduct is reported to The Consortium and may also be reported to the appropriate governmental authorities, including, but not limited to, any law enforcement officials.

7.5. Where candidates are under 18, a parent or legal guardian will be required to be physically present during the Self-Check in Process, to provide photo identification for both the candidate and the parent/guardian via camera/video for identification verification purposes. The candidate's parent/guardian will be asked to verbally confirm their consent to the UCAT test going ahead.

8. Research Database Overview

8.1. The research database contains the demographic and UCAT test data of all candidates.

8.2. All research conducted on these data requires submission of a protocol describing the questions to be addressed and analysis required, along with evidence of ethical approval if required. Only analysis approved by or on behalf of the Board is conducted.

8.3. Researchers permitted access to the research database are referred to as Approved Data Users.

8.4. In the past, some data relating to the selection of applicants to universities (obtained from UCAS) and educational data relating to students registered at universities (progression/assessment data) was incorporated into the Research Database.

8.4.1. Data obtained from UCAS is under licence allowing The Consortium to pass on an anonymised suppressed analysis of the data to Approved Data Users.

8.4.2. Universities are the data controllers of their own progression/assessment data provided for these purposes.

9. Research Database Security, Storage and Access

9.1. The Consortium has a contract with the University of Dundee Health Informatics Centre (HIC) for the hosting, development and management of the research database. Data remain wholly in the ownership of The Consortium and The Consortium retains all rights (including intellectual property) in the data. HIC processes the data on behalf of The Consortium, acting on the authorisation of the Board.

9.2. HIC Standard Operating Procedures comply with the requirements of the DPA and ensure the security of the data. HIC may not, without the written authorisation of the Board, give copies of, or allow access to the data to any third party or publish the data in any form.

9.3. HIC is ISO27001 Data Security certificated, with the scope of the certification covering all HIC processes relevant to The Consortium. HIC is externally audited annually to ensure compliance.

9.4. All Data provided to HIC is via secure encrypted mechanisms. All data transfers to the research database are logged in a document maintained by HIC.

9.5. All data are held securely at HIC, which carries out daily backups to a mirrored offsite secure server.

9.6. Access to the database is restricted to authorised HIC Data Management staff and can only be expanded to other personnel at the request of the Board. In the event of the Board granting permission for other personnel to have access to the data to undertake research/analysis on its behalf, those individuals are required to sign a Privacy Protocol.

9.7. HIC maintains data security through a number of measures:

- Clear and approved operating procedures for HIC staff with automated processes to reduce errors.
- An open access reporting system to notify of any significant events and an annual external audit of all systems and processes.
- The HIC Information Governance Committee reviews HIC's methods twice annually.

- Routine quality checking, to maintain the accuracy and integrity of datasets.
- Separate secure access-controlled areas for data processing and data storage.
- Nightly offsite mirrored back-up.

9.8. Once any research/analysis on the data is complete, data files are recovered by HIC and archived in accordance with scientific research guidelines.

9.9. Datasets are encrypted by HIC prior to transfer to Approved Data Users as per HIC standard operating procedures.

9.10. Approved Data Users normally access project data remotely via a secure HIC server hosted within the HIC "Safe Haven" environment, rather than receiving the data directly.

9.11. In some circumstances, The Consortium authorises a physical release of data. When a dataset is released, it is shared securely with the Approved Data User. Large files may be placed on the access-controlled FTP server. Only encrypted data is placed there and only the Approved Data User can access the data using an encryption key.

10. Anonymity of Research Data

10.1. Although data is received by HIC in an identifiable form, all analysis and research undertaken by or on behalf of The Consortium takes place on anonymised data. This may include the removal of names, addresses, postcodes, UCAS numbers, ID numbers, secondary school names and codes and university codes from the data made available for analysis. Certain data will not be released if it could lead to the identification of individuals. Specifically, data are not released to Approved Data Users where, by virtue of other data the Approved Data Users hold, it would be possible to de-anonymise the data provided.

10.2. The Consortium is committed to only publishing research/analysis where it is confident that individuals or subgroups of candidates cannot be identified. Published research and analysis contains aggregate data only. Any articles/papers/documents for publication are scrutinized by the Board for this purpose.

11. Data User Responsibilities

11.1. All Approved Data Users are required to maintain the security and confidentiality of project datasets in accordance with this agreement and the Data Protection Principles listed in Appendix A.

11.2. Approved Data Users may not reuse the data for purposes outside the scope of each project; share it with colleagues who are not named project Approved Data Users; attempt to link it to other datasets; or to de-anonymise it.

11.3. When the project is complete, the data and the analysis syntax used are securely archived by HIC.

11.4. Where research on data has taken place and findings are being presented for publication (in whatever form), final approval of publications rests with the Board.

12. United Kingdom Medical Education Database (UKMED)

12.1. The UK Medical Education Database (UKMED) provides a platform for collating data on the performance of UK medical students and trainee doctors across their education and future career. UKMED is achieved in partnership with data providers from across the education and health sectors, including The Consortium.

12.2. The Consortium has a data sharing agreement with the General Medical Council (GMC) in relationship to involvement in UKMED. This agreement details how the GMC meets its responsibilities in relation to the confidentiality of data and the GDPR. It also describes arrangements for consideration of proposals to undertake research/analysis on UKMED data and in particular, how decisions regarding the release of such datasets are governed.

12.3. As part of this agreement, The Consortium has agreed to supply the GMC with certain personal data to support the creation and development of the UKMED Database. Under this agreement the data is used to produce:

- reports on the progression of students and doctors in training from application to medical school through to completion of their training. These reports are aggregated, and no individuals identified.
- datasets of anonymised and pseudonymised data that may be made available to Approved Data Users for research purposes.

12.4. The GMC confirms that the processing pursuant to this Agreement is necessary for the performance of the GMC's public tasks, and that the data is only used for these purposes.

12.5. The GMC links data from The Consortium, GMC and other contributors to create UKMED. The datasets held in UKMED continue to grow and are listed in the UKMED data dictionary.

12.6. Following the creation of the UKMED database and inclusion of The Consortium Data in the database, the GMC is the sole data controller of the personal data contained within the UKMED database and determines the purposes for the use and processing of the personal data and therefore shall have legal responsibility for it.

12.7. The Consortium is a member of the UKMED Advisory Board.

12.8. The Data Sharing Agreement with the GMC may be terminated at any time.

12.9. Further information regarding UKMED can be found here.

13. Data subject rights

13.1. Where processing of personal data is based on consent, consent can be withdrawn at any time. These rights can be exercised at any time by contacting The Consortium at ucat@nottingham.ac.uk. Candidates have the right:

13.1.1. Not to have their personal data used for marketing purposes. The Consortium will inform candidates (before collecting these data) if they intend to use data for such purposes or if they intend to disclose information to any third party for such purposes.

13.1.2. Where personal data is processed on the basis of legitimate interests, to object to such processing, provided that there are no compelling reasons for that processing.

13.1.3. To ask The Consortium not to process their personal data for scientific or historical research purposes, where relevant, unless the processing is necessary in the public interest.

13.1.4. To request access to personal information held about them.

13.1.5. To ask for the information The Consortium holds about them to be rectified if it is inaccurate or incomplete.

13.1.6. To ask for data to be erased provided that:

- the personal data is no longer necessary for the purposes for which it was collected;
- or they withdraw consent (if the legal basis for processing is consent);
- or they exercise their right to object as set out below, and there are no overriding legitimate grounds for processing;
- or the data is unlawfully processed;
- or the data needs to be erased to comply with a legal obligation;
- or the data is children's data and was collected in relation to an offer of information society services.

13.1.7. To ask for the processing of that information to be restricted if the accuracy of that data is contested, the processing is unlawful, the personal data is no longer necessary for the purposes for which it was collected or the right to object is exercised (pending verification of whether there are legitimate grounds for processing).

13.1.8. To ask for data portability if the processing is carried out by automated means and the legal basis for processing is consent or pursuant to a contract.

13.2. Should any issues, concerns or problems arise in relation to candidate data, or if they wish to notify The Consortium of data that is inaccurate, then The Consortium may be contacted using the details below. If they are not satisfied, they have the right to lodge a complaint with the relevant supervisory authority, which is the Information Commissioner's Office (ICO) in the UK, at any time. The ICO's contact details are available here: https://ico.org.uk/concerns/.

14. Data Breach

14.1. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

14.2. All information users (including UCAT staff, PPA and others handling data on the Consortium's behalf) are responsible for reporting actual, suspected, threatened or potential information security incidents, which includes personal data breaches. Any unmitigated breach that affects the rights and freedoms of an individual must be reported to the ICO by the Information Compliance Team no later than 72 hours after the Consortium becomes aware of it, so prompt reporting is essential.

14.3. All data breaches are logged. Where a data breach is identified, efforts will be made to rectify or contain the breach.
14.4. Where individuals have received the personal data of others in error, they would be apologised to, asked to delete the material without sharing it further and asked to confirm the deletion of the material.
14.5. The UCAT Consortium Office will determine whether it is appropriate to notify the affected data subject that a breach has occurred. If appropriate, the data subject will be apologised to and notified of the nature of the data breach.
14.6. Any report of a data breach will lead to a review of relevant processes and policies to prevent similar occurrences in the future.

15. Changes to this Privacy Policy

From time to time, The Consortium may revise this Privacy Policy to reflect industry initiatives, changes in law or technology, or changes in policies and practices regarding personal data processed. If significant revisions are made to the way personal data is processed, then notice of those changes will be provided by an announcement on The Consortium homepage and notices on relevant social media platforms.

16. Requests for Information

Individuals may submit a general request for information from the UCAT Consortium as a Freedom of Information request or request access to personal information held by the UCAT Consortium under a Subject Access Request. All requests will be handled in accordance with guidance issued by the Information Commissioner's Office.

17. Contact us

Questions comments and requests regarding this privacy notice are welcomed and should be addressed to ucat@nottingham.ac.uk.

Rachel Greatrix, Chief Operating Officer, UCAT Consortium

Appendix A: The 7 Data Protection Principles

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;

2. Personal data shall be 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;

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Personal data shall be 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;

5. Personal data shall be 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;

6. 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;

7. The controller shall be responsible for, and be able to demonstrate compliance with the principles above.