UCAT DATA PRIVACY POLICY 2024

The UCAT Consortium has a number of 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. Any substantial amendments to policies are considered in the light of their impact on EDI.

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 VUE (PVUE) deliver and develop the UCAT test on behalf of The Consortium. The UCAT test is delivered on computer (at PVUE test centres in the UK and worldwide) and may also be Online Proctored.

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

1.5. 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.

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

2. Overview

2.1. 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). This document is structured as follows:

- Section 4 describes why we need to collect candidate personal data.
- Section 5 describes what data we collect from candidates. This section also explains how data is shared between The Consortium, PVUE and Consortium Universities.
- Section 7 describes additional data collected from candidates taking the Online Proctored UCAT test.
- Sections 8-13 explain how data is used in research and analysis and the security measures in place.
- In Section 14 the rights of candidates as data subjects are explained.

2.2. When registering to take the UCAT test, candidates are directed to both the PVUE Privacy Policy and The Consortium Data Privacy Policy.

2.3. Analysis and research on these data by or on behalf of The Consortium, is undertaken on anonymous data and used in research to further the core objectives of The Consortium.

Given these conditions, The Consortium does not need to seek individual consent to use data as described in this document.

2.4. 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.

3. Information from Children

3.1. 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.

3.2. 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.

4. Why does The Consortium need candidate data?

4.1. 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 the marketing and business strategy;
- understand the effectiveness of The Consortium's research; and
- defend against or exercise legal claims, investigate complaints and respond to queries.

4.2. 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;
- 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.

5. What data does The Consortium collect?

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

5.2. 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 or delivery of UCAT test results and are never used for broader marketing purposes.

5.3. Additional 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).

5.4. '**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.

5.5. When candidates apply for a **UCAT bursary**, they provide personal data and upload evidence to support their application. These data are retained until the end of the calendar year for reporting and accounting purposes. 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. By submitting an application and providing supporting evidence, candidates agree to these data being used for the administration of the bursary scheme. Where candidates have provided evidence that includes the data of any third party, they will be asked to confirm that they have obtained necessary consent.

5.6. In order to assess required **access arrangements/accommodations**, candidates are asked to provide supporting evidence that may contain their personal information and/or that of a third party. This evidence is used by The Consortium for the purpose of assessing needs. The Consortium may also need to communicate details to PVUE in order for PVUE to make any agreed booking arrangements. When providing evidence, candidates will be asked to consent to these data being used for this purpose. If candidates have provided evidence that includes the data of any third party, they will be asked to confirm they have obtained necessary consent. Any data received in relation to making access arrangements are retained for the duration of the relevant admissions cycle (usually until September the following year). The Consortium does not share information regarding access arrangements/accommodations with Consortium Universities without candidate agreement.

5.7. 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.

5.8. In the provision of **customer service** and for the performance of the contract, The Consortium and PVUE 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 PVUE or in the legitimate interests of The Consortium and PVUE. PVUE retains these data in accordance with their privacy policy.

5.9. When **attending a test centre** to undertake the exam, PVUE collects a photo image of candidates, 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 PVUE and is subject to PVUE's retention period. The Consortium may ask PVUE to share this information where investigation is required.

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

5.11. 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.

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;

6.1.2. and other partner Consortium Universities which candidates apply to or indicate they intend to apply to (when creating their UCAT account).

6.2. PVUE on behalf of UCAT has an agreement with UCAS to share candidate data to support the delivery of UCAT test results to Consortium Universities. PVUE provides UCAS with candidate data which is used by UCAS to match candidates to any applications they have made through UCAS to courses at Consortium Universities requiring candidates to take the UCAT test as part of their selection criteria ("UCAS choices"). UCAS provides PVUE with candidate UCAS choices which allows The Consortium to provide Consortium Universities 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 is able to 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 are not able to 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. As indicated above 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 to them.

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 the Pearson VUE's Privacy and Cookies Policy to support their testing experience.

7.2. During an automated check-in process, candidates will need to 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. Pearson VUE 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. Pearson VUE, 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 Pearson VUE on behalf of The Consortium (the data controller). 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. All research conducted on 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.

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

8.3. 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.

8.3.1. Data obtained from UCAS is under licence, the requirements of which are observed by the Board in its use of the data. For clarity, this allows The Consortium to pass on an anonymised suppressed analysis of the data to approved researchers, including members of The Consortium.

8.3.2. Universities are the data controllers of their own progression/assessment data. The Consortium has entered into agreements with some universities regarding the provision and use of progression data. Whether universities are able to provide progression or other data to The Consortium is governed by their own registration agreement with students, which is underpinned by their policy agreement with the Information Commissioner's Office. It is likely that such policy agreements refer to research on or analysis of data and therefore allow for the provision of progression or other data.

8.4. In the future, further data may be collected, for example additional selection data such as Multiple Mini Interview (MMI) scores, foundation year data or postgraduate data. This policy will be updated as required. The Consortium would enter into an agreement regarding the provision and use of such data. Agreements would specify whether the data provided is solely for the purpose of a specific project or whether it can be held over a longer period.

9. Research Database Security, Storage and Access

9.1. The Consortium has entered into 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. These arrangements are outlined in greater detail in this document. 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 involved with The Consortium. HIC is externally audited annually to ensure compliance.

9.4. All Data provided to HIC, from PVUE and universities 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 currently 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 all 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.

10. Anonymity of Research Data

10.1. As outlined above, 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. Where necessary, certain data may not be released if it could lead to the identification of individual students. Specifically, data are not released to researchers where, by virtue of other data they hold on applicants or students, 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.

10.3. The Consortium is not seeking to publish research/analysis where individual universities are identified by name, unless otherwise agreed. Where compatible with effective presentation of data, information that would identify individual universities is omitted. In the event of research/analysis being such that it is likely that individual universities could be identified, the relevant universities are informed in advance. Any decision to publish such work would be made by the Board.

11. Transfer of Data to Researchers

11.1. Datasets are encrypted by HIC prior transfer to researchers as per HIC SOPs.

11.2. Researchers normally access project data remotely via a secure HIC server hosted within the HIC "Safe Haven" environment, rather than receiving the data directly.

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

12. Data User Responsibilities

12.1. 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.

12.2. 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.

12.3. When the project is complete, the data and the analysis syntax used are securely archived by HIC.
12.4. 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.

13. United Kingdom Medical Education Database (UKMED)

13.1. 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.
13.2. The Consortium has a data sharing agreement with the General Medical Council (GMC) in relationship to involvement in the United Kingdom Medical Education Database (UKMED) project. 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.
13.3. 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 researchers.

13.4. 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.
13.5. 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.
13.6. 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.
13.7. The Consortium is a member of the UKMED Advisory Board.
13.8. The Data Sharing Agreement with the GMC may be terminated at any time.
13.9. Further information regarding UKMED can be found here.

14. Data subject rights

14.1. 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:
14.1.1. 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.
14.1.2. 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.
14.1.3. 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.
14.1.4. To request access to personal information held about them.
14.1.5. To ask for the information The Consortium holds about them to be rectified if it is inaccurate or incomplete.
14.1.6. 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.

14.1.7. 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).

14.1.8. 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.

14.2. 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. In the event that 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/.

15. Data Breach

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

15.2. All information users (including UCAT staff, Pearson VUE 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.

15.3. All data breaches are logged. Where a data breach is identified, efforts will be made to rectify or contain the breach.

15.4. Where individuals have received the personal data of others in error, they would be apologised to, and asked to delete the material without sharing it further and asked to confirm the deletion of the material.

15.5. The UCAT Office will determine whether it is appropriate to notify the affected data subject that a breach has occurred. If appropriate, the data subject should be apologised to and notified of the nature of the data breach.

15.6. Any report of a data breach will lead to a review of relevant processes and policies to prevent similar occurrences in the future.

16. 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 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.

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