DATA PRIVACY POLICY 2023

1. Introduction

1.1. This policy applies to data collected by The UCAT Consortium relating to potential or actual test candidates. References in this Privacy Policy to "we", "us", "UCAT Consortium" and "The Consortium" are to The UKCAT Consortium (company number 05620264), registered office UK Clinical Aptitude Test, D 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 used by Universities in the UK as part of selection processes for healthcare programmes. The organisation is managed by a Board elected from representatives of participating Universities.

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

1.4. The UCAT 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 your personal data are handled in accordance with the Act.

2. Overview

2.1. This policy provides information regarding data the UCAT Consortium holds in relation to test takers, 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 your personal data.
- Section 5 describes what data we collect from you. This section also explains how data is shared between the Consortium, PVUE and Universities.
- Section 6 describes additional data collected from those taking the Online Proctored test.
- Sections 7-12 explain how data is used in research and analysis and the security measures in place.
- Section 13 lists the different agreements in place around the use of your data.
- In Section 14 your rights as a data subject are explained.

2.2. When registering to take the test, you will be 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 your 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. If you are under 18, please be sure to read this Privacy Policy with your parent(s) or legal guardian(s) and ask questions about things you do not understand.

4. Why does the Consortium need your 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 tests;
- study how test takers 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 your data to:

- administer tests (including data required to book a test, to verify your details and to communicate test results to participating medical and dental schools);
- consider your eligibility for access arrangements;
- investigate complaints or incidents have that occurred during testing;
- investigate allegations of misconduct;
- undertake internal analysis of how the tests work including looking at the reliability of tests and whether they favour particular subgroups;
- undertake and support research aimed at improving the 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. This data is used for the Consortium's legitimate interests in assisting with the administration of the test 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 you in relation to the administration of the test or delivery of results and are never be used for broader marketing purposes.

5.3. `**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 test does not discriminate against or in favour of those from particular ethnic origins. Special categories of personal data may also be provided to the Consortium where a bursary or access arrangements application is made. If used in research and analysis, such data are fully anonymised.

5.4. The **data passed to medical and dental schools** are test result data (including personal identifiers) which schools have access to for test takers who apply to them through UCAS.

5.5. If you apply for a **UCAT bursary**, you will provide personal data and upload evidence to support your application. These data are retained until the end of the calendar year for reporting and accounting purposes. If you are awarded a bursary, this is flagged to your chosen universities at results delivery. For clarity, 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, you agree to these data being used for the administration of the bursary scheme. Where you have provided evidence that includes the data of any third party, you will be asked to confirm that they have obtained necessary consent.

5.6. In order to assess required **access arrangements/accommodations**, you will be asked to provide supporting evidence that may contain your 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, you will be asked to consent to these data being used for this purpose. If you have provided evidence that includes the data of any third party, you will be asked to confirm you 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 universities without your agreement.

5.7. On occasion, the Consortium may **survey** test takers to obtain information to enhance the test taker experience and/or contribute to research projects. For research purposes, the Consortium may link survey data to test and your data. Your informed consent to take part in any survey will be obtained. You 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 your information with each other to effectively deal and respond to issues you may encounter in the administration of the test. Personal data processed is pursuant to a contract between you 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 you, your signature and CCTV images for the purposes of safety, security and fraud prevention. You will be asked to present a government issued ID with photo and signature and this information is used to confirm your identity. This is necessary for the performance of the contract between you 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 your information by clicking here.

6. What additional data is required if you take the Online-Proctored test?

6.1. If you take the online-proctored test you will be asked to agree to the terms set out in the Pearson VUE's Privacy and Cookies Policy to support your testing experience.

6.2. During an automated check-in process, you will need to upload a photo of yourself and share your 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 your 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.

6.3. You will be asked to acknowledge and agree to video and audio recording of your entire testing session and to the processing of such personal information and test data by Pearson VUE on behalf of the UCAT Consortium (the data controller). Video and audio recording are used for purposes of identity verification, remote observation, incident resolution, such as fraud prevention, test security, and for the integrity of the test and the testing process.

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

6.5. If you 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 you and them via camera/video for identification verification purposes. Your parent/guardian will be asked to verbally confirm their consent to your test going ahead.

7. Research Database Overview

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

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

7.3. Data relating to admissions on applicants to participating medical and dental schools in the UK and educational data relating to medical and dental students registered at medical and dental schools in the UK may also be incorporated into the Research Database.
7.4. Progression (assessment) data collected from medical and dental schools contain student identifiers to enable confirmation of matching. Once data has been matched to the research database, the originals are stored in a secure archive.
7.5. When releasing data for research purposes, a unique identifier is applied to ensure pseudonymisation.
7.6. In the future, further data may be collected, for example additional admissions data such as Multiple Mini Interview (MMI) scores, foundation year data or postgraduate data. This policy will be updated as required.

8. Research Database Security, Storage and Access

8.1. 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.
8.2. 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.
8.3. 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.
8.4. All Data provided to HIC, from PVUE, medical and dental schools is via secure encrypted mechanisms. All data transfers to the research database are logged in a document maintained by HIC.
8.5. All data are held securely at HIC, which carries out daily backups to a mirrored offsite secure server.
8.6. 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.
8.7. 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.

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

9. Anonymity of Research Data

9.1. 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 medical schools

where, by virtue of other data they hold on applicants or students, it would be possible to de-anonymise the data provided.

9.2. 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.

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

10. Transfer of Data to Researchers

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

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

10.3. In some circumstances, the Consortium authorises a physical release of data. When a dataset is released, it is emailed (encrypted) to the researcher. If it is too large to be emailed it is 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.

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 Consortium 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 entered into a data sharing agreement with the GMC to supply the GMC with certain personal data to assist with the creation 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.

12.3. 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.

12.4. 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.

12.5. Following the creation of the UKMED database and inclusion of 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.

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

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

12.8. Further information regarding UKMED can be found here.

13. Agreements in Place

13.1. 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.

13.2. UCAS and Consortium Universities are the data controllers of data transferred to the Consortium by UCAS regarding your University choices, examination results and final destinations. 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.

13.3. Consortium members (Universities) are the data controllers of their own progression (assessment) data. The Consortium has entered into agreements with consortium members regarding the provision and use of progression data. Universities are provided with a copy of this Privacy Policy to fully inform them of the uses and security in place for data provided.

13.4. Consortium members or other Universities may wish to utilise their own data within a research project (e.g. MMI data). Those Universities would remain data controllers of such data. The Consortium enters into an agreement regarding the provision and use of such data. Such an agreement specifies whether the data provided is solely for the purpose of a specific project or whether it can be held over a longer period.

13.5. 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.

13.6. 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.

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. You have the right:

14.1.1. Not to have your personal data used for marketing purposes. The Consortium will inform you (before collecting your data) if they intend to use your data for such purposes or if they intend to disclose your 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 your 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 you.

14.1.5. To ask for the information the Consortium holds about you 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 you withdraw consent (if the legal basis for processing is consent);
- or you exercise your 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 your data, or if you wish to notify the Consortium of data that is inaccurate, then the Consortium may be contacted using the details below. In the event that you are not satisfied, you 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. 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.

16. 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;

- must not deceive or mislead
- must state the purpose of the processing
- must provide your identity
- must have consent of the data subject – cannot infer this from a lack of response
- must specify time period of consent
- must have appropriate safeguards for data
- must obtain consent from data subjects for processing if data provided by a third party

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;

- Must identify purposes for which data is being processed
- Must ensure purposes are compatible with information given to data subjects and to the Information Commissioner's Office (www.ico.gov.uk)
- Must not further process if purposes are not compatible with consent or notification to ICO without resolving conflicts

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

- Must establish what is collected and why
- Must audit data holding against need – minimum information must be collected – do not collect 'just in case'
- Must establish effective data retention and disposal policies
- Must establish policies and procedures to test new and modified data collection against the principles

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;

- Must establish methods to validate the source of data
- Must establish policies and procedures to keep data up–to-date
- Must establish policies and procedures to correct or mark as incorrect any disputed data

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;

- Must establish policies and procedures review why you are retaining data – e.g. current use, audit/ legal purposes, research purposes
- Must delete data that is no longer needed

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;

- Rights of data subjects include:
- Right to be told that their personal data is being processed and for what purpose
- Right to obtain a copy of their personal data

- Right to prevent the use of their data for direct marketing purposes
- Right to be told to whom the data will be disclosed
- Right to prevent processing which may cause substantial damage or distress to the data subject
- Right to have explained the logic behind any decision taken on the basis of the processing of the data
- Must manage operations to ensure that data subjects can exercise their rights properly and fully

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