DATA PRIVACY POLICY (March 2019)

This policy applies to data collected by The UCAT Consortium relating to candidates who have taken the test.

References in this Privacy Policy to "we", "us" 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.

The Consortium is committed to achieving greater fairness in selection to medicine and dentistry and to widening participation in medical and dental training of under-represented social groups. Through an ongoing programme of research, The Consortium is seeking to identify the characteristics in applicants which will make them good dentists and doctors and thus improve the quality of those who enter the professions with the ultimate aim of improving patient care.

The Consortium is a charity and private limited company managed by a Board elected from representatives of participating medical and dental schools.

Tests are delivered annually to approximately 25,000 candidates. The test is delivered on computer at PV test centres throughout the UK and worldwide.

1. Introduction

1.1. This policy provides information regarding data The Consortium holds in relation to candidates who have taken tests, where they are derived from and how they are used in accordance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

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

1.3. At registration candidates are referred to both the PV Privacy Policy and the Consortium Data Privacy.

1.4. 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 the individual consent of candidates to use their data as described in this document.

1.5. The Consortium's policy is to retain candidate 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 which has been anonymised for longer than this period to allow The Consortium to carry out its research objectives.

2. Why does the Consortium need candidate data?

2.1. to administer the test (including data required to book the test, to verify candidate details and to communicate test results to participating medical and dental schools);

2.2. to undertake analysis of the internal reliability of tests (i.e. is it a fair test and does it favour particular demographics of candidates);

2.3. to undertake and support research aimed at improving the test including research into the predictive validity of the test with regards to medical and dental schools performance and performance beyond undergraduate medical and dental training; and

2.4. to undertake and support research more broadly related to admissions to medicine and dentistry that relates to the core objectives of the Consortium.

3. What data does the Consortium collect from candidates?

3.1. At registration for the test, PV collects personal data from candidates on the Consortium's behalf. This data is used for the Consortium's legitimate interests in assisting with the administration of the test, to review the 'fairness' of the test and ultimately in research studies.

3.2. Data collected from candidates includes emails, phone numbers and mobile phone numbers. These may be used by the Consortium (or PV on behalf of the Consortium) to contact candidates. Such communications will be related to the administration of the test or delivery of results and will never be used for broader marketing purposes.

3.3. 'Special category data' (as defined by the Information Commissioner) collected by the Consortium includes ethnicity data collected at candidate registration as part of the socio-economic information. These data are used to ensure that the test (including specific elements of the test) does not discriminate against or in favour of candidates 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 by the candidate. If used in research and analysis such data will be fully anonymised.

3.4. The data passed to medical and dental schools are test result data (including personal identifiers) which schools receive for those candidates who have applied to them through UCAS.

3.5. When a candidate applies for a bursary they provide personal data and upload documentation to support their application. These data will be retained until the end of the calendar year for reporting and accounting purposes. If a candidate is awarded a bursary, this will be flagged to their chosen universities at results delivery. For clarity, universities are informed which of their candidates have been awarded a bursary but they do not have access to any other data provided by the candidate in their bursary application. Candidates are advised of this when submitting their application. 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 are asked to confirm that they have obtained necessary consent.

3.6. In order to assess required access arrangements/accommodations, candidates are asked to provide supporting evidence which may contain their personal information or that of a third party. This evidence is used by the Consortium for the purpose of assessing candidate needs. The Consortium may also need to communicate details to PV in order for PV to make any agreed booking arrangements. When providing evidence candidates are asked to consent to these data being used for this purpose. Where candidates have provided evidence that includes the data of any third party they are asked to confirm they have obtained the necessary consent. Any data received in relation to making access arrangements will be retained for the duration of the relevant admissions cycle (usually August the following year). On occasion, the Consortium may need to share information regarding access arrangements/accommodations with the Universities a candidate has applied to.

3.7. On occasion the Consortium may undertake surveys of candidates to obtain information which may be used to enhance the candidate experience and/or contribute to research projects. Sometimes, for research purposes, the Consortium

link survey data to test and candidate data. The informed consent of candidates to take part in any survey will always be obtained. Candidates will have the option to not take part in such surveys. Researchers using survey data will only have access to anonymised datasets as outlined below.

3.8. In the provision of customer service and for the performance of the contract with candidates, the Consortium and PV may share candidate information with each other in order to effectively deal and respond to issues candidates may encounter in the administration of the test. Personal data processed will be pursuant to a contract between PV and the candidate or in the legitimate interests of the Consortium and PV. PV will retain these data in accordance with their privacy policy.

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

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

3.10.1. carry out the administration of tests;

3.10.2. study how candidates use the Consortium's services to inform the marketing and business strategy;

3.10.3. understand the effectiveness of the Consortium's research; and

3.10.4. defend against or exercise legal claims, investigate complaints and respond to candidate queries.

3.11. Please refer to the PV's separate privacy policy to understand how they will use candidate information by clicking here.

4. Research Database Overview

4.1. 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 where necessary. Only analysis approved by or on behalf of the Board will be conducted.

4.2. The research database contains demographic, admissions and educational data on applicants to, and medical and dental students registered at participating medical and dental schools in the UK. The data collected provide the Consortium with an effective, reliable mechanism for:

4.2.1. The verification of the internal reliability of tests (i.e. is it a fair test and does it favour particular demographics of candidates) through research and analysis

4.2.2. The establishment of the predictive validity of tests with regards to medical and dental schools performance through research and analysis

4.2.3. The establishment of the predictive validity of tests with regards to postgraduate medical and dental performance through research and analysis

4.2.4. Undertaking research related to admissions to medicine and dentistry that relates to the core objectives of the Consortium.

4.3. Progression 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.
4.4. When releasing data for research purposes, a unique identifier is applied to ensure pseudonymisation.
4.5. 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.

5. Research Database Security, Storage and Access

5.1. 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. 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.
5.2. HIC is ISO27001 Data Security certificated, with the scope of the certification covering all HIC processes involved with the Consortium. HIC is externally audited twice annually to ensure compliance.
5.3. All Data provided to HIC, from PV, medical and dental schools will be via secure encrypted mechanisms, e.g. ftp.
5.4. Data imports from UCAS are downloaded to HIC from an open site in an encrypted, compressed file. Passwords for this purpose are exchanged by telephone.
5.5. Progression data from medical and dental schools are requested in an excel spreadsheet (candidates are identified by unique identifiers only) and provided to the Consortium. Data transfers are password protected and passwords for this purpose exchanged by telephone. Data are checked for completeness and transferred to HIC through a secure method. Original data are to be encrypted, archived and stored for a period of five years (to be reviewed) before being deleted. HIC has developed secure mechanisms to allow the Consortium, or medical schools themselves, to upload data directly to HIC.
5.6. All data transfers to the research database are logged in a document maintained by HIC.
5.7. All data is held securely at HIC, which carries out daily backups to a mirrored offsite secure server.
5.8. 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 would be required to sign a Privacy Protocol which would outline the security measures the Consortium would expect the individual to put in place with regard to the storage of the data.
5.9. HIC maintains data security through a number of measures:

5.9.1. Clear and approved operating procedures for HIC staff with automated processes to reduce errors

5.9.2. An open access reporting system to notify of any significant events and an annual external audit of all systems and processes
5.9.3. The HIC Information Governance Committee reviews HIC's methods twice annually
5.9.4. Routine quality checking, to maintain the accuracy and integrity of datasets
5.9.5. Separate secure access-controlled areas for all data processing and data storage
5.9.6. Nightly offsite mirrored back-up

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

6. Anonymity of Research Data

6.1. As outlined above, data is received by HIC in an identifiable form. The Consortium is committed to ensuring that at no point can candidates be identified within published analysis/research that has taken place on its data. As such, 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 (such as gender, ethnicity and university of study combined). Specifically data will not be 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. Published research/analysis will contain aggregate data only.

6.2. The Consortium is committed to only publishing research/analysis where it is confident that individual candidates or subgroups of candidates cannot be identified. Published research/analysis will contain aggregate data only. Any articles/papers/documents for publication are scrutinized by the Board for this purpose. In addition, prior to publication of any research/analysis which includes UCAS data, UCAS's agreement to publication must be sought.

6.3. 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 which would identify individual schools will be omitted. In the event of research/analysis being such that it is likely that individual medical and dental schools could be identified then the relevant schools will be informed in advance. Any decision to publish such work would be made by the Board.

7. Transfer of Data to Researchers

7.1. All datasets will be encrypted by HIC prior to being transferred to researchers, as per HIC SOPs.

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

7.3. In some circumstances, the Consortium will authorise a physical release of data. When a dataset is released it will be emailed (encrypted) to the researcher. If it is too large to be emailed it will be placed on the access-controlled FTP server. Only

encrypted data will be placed there and only the researcher will be able to access the data using their encryption key.

8. Data User Responsibilities

8.1. All Approved Data Users are required to maintain the security and confidentiality of their project datasets in accordance with this agreement and the Data Protection Principles listed in Appendix A.
8.2. Approved Data Users will 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.
8.3. When the project is complete the data and the analysis syntax used will be securely archived by HIC.
8.4. Publication of Findings
8.5. 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.

9. Agreements in Place

9.1. Under Data Protection Legislation, the Consortium is the data controller of data collected by PV on behalf of the Consortium. In line with the requirements of the DPA the Consortium has a written agreement with PV (Agreement for the Supply of Test Delivery and Development Services) which outlines PV's responsibilities in collecting, holding and transferring data on the Consortium's behalf.
9.2. UCAS and Consortium Universities are the data controllers of data transferred to the Consortium by UCAS regarding candidate 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.
9.3. Consortium members (Universities) are the data controllers for their own progression data. The Consortium will enter into an agreement with each consortium member regarding the provision and use of progression data. Members are provided with a copy of this Privacy Policy to fully inform them of the uses and security in place for data provided.
9.4. 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 will enter into an agreement regarding the provision and use of such data. Such an agreement will specify whether the data provided is solely for the purpose of a specific project or whether it can be held over a longer period.
9.5. Whether Universities are able to provide progression or other data to the Consortium will be governed by their own registration agreement with students, which will be underpinned by their policy agreement with the Information Commissioner's Office. It is likely that such policy agreements will refer to research on or analysis of data and will therefore allow for the provision of progression or other data.
9.6. 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. Further information regarding UKMED can be found in section 10 below.

10. United Kingdom Medical Education Database (UKMED)

10.1. 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.

10.2. 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 will be used to produce:

10.2.1. reports on the progression of students and doctors in training from application to medical school through to completion of their training. These reports will be aggregated and no individual will be identified.

10.2.2. datasets of anonymised and pseudonymised data which may be made available to researchers.

10.3. 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 will only be used for the purpose of research.

10.4. The GMC will link Consortium Data to GMC data and data from other contributors to create the UKMED database. The datasets held in UKMED will continue to grow and are listed in the UKMED data dictionary.

10.5. Following the creation of the UKMED database and inclusion of Consortium Data in the database, the GMC will be the sole data controller of the personal data contained within the UKMED database and will determine the purposes for the use and processing of the personal data, and therefore shall have legal responsibility for it.

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

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

10.8. Further information regarding UKMED can be found at www.ukmed.ac.uk

11. Data subject rights

11.1. 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:

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

11.1.2. 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;

11.1.3. 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;

11.1.4. To request access to personal information held about themselves;

11.1.5. To ask for the information the Consortium holds about themselves to be rectified if it is inaccurate or incomplete;

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

11.1.6.1. the personal data is no longer necessary for the purposes for which it was collected;

11.1.6.2. or they withdraw consent (if the legal basis for processing is consent);

11.1.6.3. or they exercise their right to object as set out below, and there are no overriding legitimate grounds for processing;

11.1.6.4. or the data is unlawfully processed;

11.1.6.5. or the data needs to be erased to comply with a legal obligation;

11.1.6.6. or the data is children's data and was collected in relation to an offer of information society services.

11.1.7. 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);

11.1.8. 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.

11.2. Should any issues, concerns or problems arise in relation to candidate data, or if candidates wish to notify the Consortium of data that is inaccurate, then the Consortium may be contacted using the details below. In the event that candidates are not satisfied, candidates 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/.

12. 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.

13. Contact us

Questions comments and requests regarding this privacy notice are welcomed and should be addressed to UCAT Consortium, D Floor, The Medical School Queen's Medical Centre, Nottingham NG7 2UH or 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