DATA PRIVACY POLICY (Updated June 2017)

This policy applies to data collected by The UKCAT Consortium relating to candidates who have taken the test. This document has been produced in line with legal advice obtained by the UKCAT Board in July 2009 from Pinsent Masons LLP. The statement has been revised in reference to the Information Commissioner's Office code of practice Anonymisation: Managing Data Protection Risk.[1]

1. Introduction

1.1. The UKCAT Consortium is committed to achieving greater fairness in selection to medicine and dentistry and to the widening participation in medical and dental training of under-represented social groups. Through an ongoing programme of research, The UKCAT 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.

1.2. The UKCAT Consortium is a charity and private limited company managed by a Board elected from representatives of participating medical and dental schools. The Board is answerable to those schools who meet twice a year.

1.3. Tests are delivered annually to approximately 25,000 candidates. The test is delivered by The UKCAT Consortium's business partner, Pearson VUE (PV), on line at PV test centres throughout the UK and worldwide in a further countries. Candidate test results are passed to the medical and dental schools they apply to in order that test results might contribute to the admissions process.

1.4. This policy provides information regarding the data we hold in relation to candidates who have taken tests, where they are derived from and how they are used.

1.5. The UKCAT Consortium is registered as a data controller with the UK Information Commissioner's Office for the purposes of the Data Protection Act 1998. The UKCAT Consortium is committed to ensuring that the personal data of candidates who take its test are handled in accordance with the Act.

2. What Data does UKCAT collect from candidates?

2.1. At registration for the test, Pearson VUE collects personal data from candidates on The UKCAT Consortium's behalf. This data assists with the administration of the test and provide data that can be used to review the 'fairness' of the test and can be used ultimately in research studies relating to test development or wider issues in admissions to medicine and dentistry.

2.2. Data collected from candidates includes emails, phone numbers and mobile phone numbers. These may be used by The UKCAT Consortium or Pearson VUE on behalf of The UKCAT 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.

[1] http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/anonymisation.aspx

2.3. When a candidate applies for a bursary they provide personal data and upload documentation to support their application. This data is retained for a maximum of three years. 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.

2.4. When a candidate requires exam access arrangements or asks for consideration of mitigating circumstances they may provide personal data to support their request. This data is retained for a maximum of three years. Details may be communicated to consortium universities and medical or dental schools may request sight of any evidence supplied.

2.5. On occasion UKCAT may undertake surveys of candidates to obtain information from them which may be used to enhance the candidate experience and/or contribute to research projects. Sometimes for research purpose UKCAT will need to link survey data to test and candidate data. Candidate consent to take part in such surveys 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.

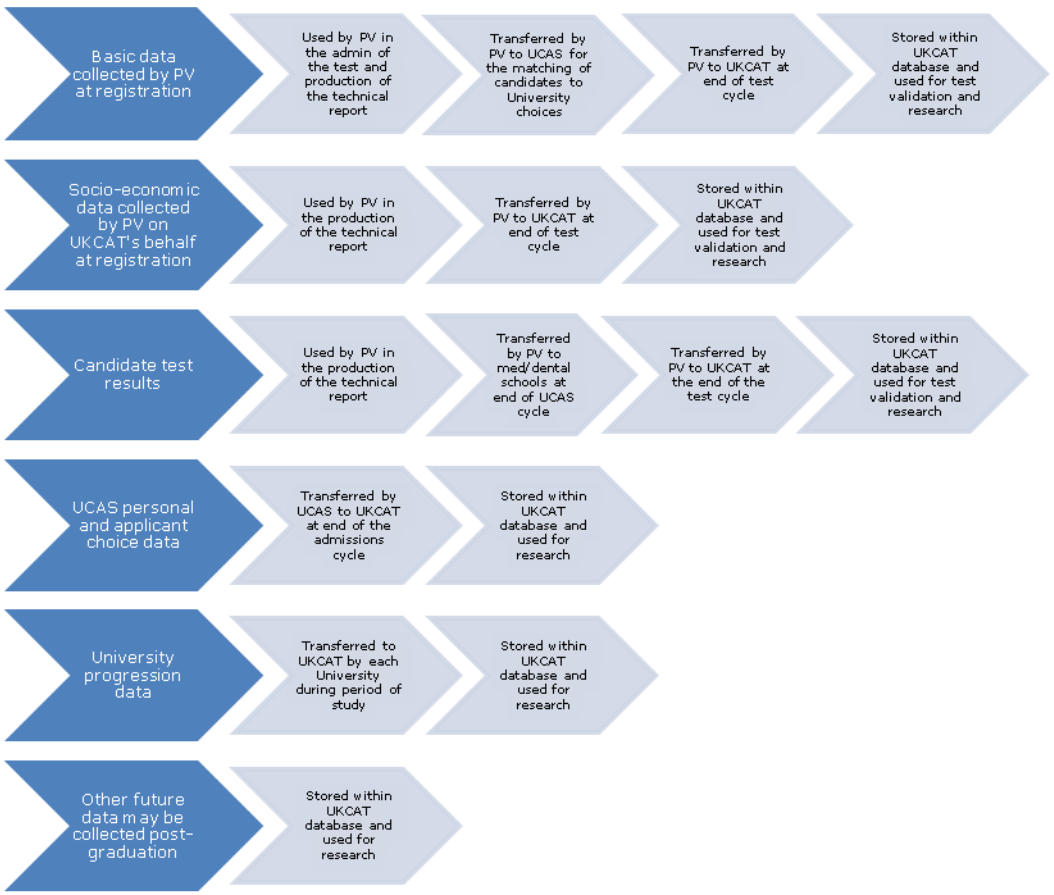
3. Overview of the UKCAT Consortium Database

3.1. The UKCAT Consortium 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 UKCAT Consortium with an effective, reliable mechanism for:

- The administration of tests (i.e. to verify candidate details and to be able to communicate correct test results to participating medical and dental schools)
- 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
- The establishment of the predictive validity of tests with regards to medical and dental schools performance through research and analysis
- The establishment of the predictive validity of tests with regards to postgraduate medical and dental performance through research and analysis
- Undertaking research related to admissions to medicine and dentistry that relates to the core objectives of The UKCAT Consortium (outlined above 1.1).†

† All research conducted on The UKCAT 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.

3.2. The table below summarises the data collected by The UKCAT Consortium and on its behalf by Pearson Vue, the flow of these data and the uses made of them.



3.3. The only 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.

3.4. The only 'sensitive personal data' (as defined by the Information Commissioner) collected by The UKCAT Consortium are 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. If used in research and analysis such data will be fully anonymised.

3.5. Progression data collected from medical and dental schools contain student identifiers to enable confirmation of matching. Once data have been matched to the The UKCAT Consortium database the originals will be stored in a secure archive.

3.6. When releasing data for research purposes, a unique identifier is applied to ensure that research and analysis conducted on the database is anonymised.

3.7. 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 date. This policy will be updated as required.

4. Agreements in Place

4.1. Under the Data Protection Act 1998 (DPA) The UKCAT Consortium is the data controller of data collected by PV on behalf of The UKCAT Consortium. In line with the requirements of the act The UKCAT Consortium has a written agreement with PV (The Professional Test Development and Delivery Services Agreement)

which outlines PV's responsibilities in collecting, holding and transferring data on The UKCAT Consortium's behalf.

4.2. UCAS and Consortium Universities are the data controllers of data transferred to The UKCAT Consortium by UCAS regarding candidate choices, examination results and final destinations. To date the data obtained from UCAS is under licence, the requirements of which are observed by the Board of UKCAT in its use of the data. For clarity this allows UKCAT to pass on an anonymised suppressed analysis of the data to approved researchers, including members of the UKCAT Consortium.

4.3. Consortium members (Universities) are the data controllers for their own progression data. The UKCAT 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.

4.4. 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 UKCAT 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.

4.5. Whether Universities are able to provide progression or other data to The UKCAT 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.

4.6. The UKCAT 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 Data Protection Act. 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 9 below.

5. Information to Candidates

5.1. At registration for the test, the attention of candidates is drawn to the PV Privacy Policy. In addition this The UKCAT Consortium Data Privacy Statement outlines the reasons for the collection of data and the nature of research and analysis which may take place on these data. This statement is also drawn to the attention of candidates at registration.

5.2. Analysis and research on these data by or on behalf of The UKCAT Consortium, is undertaken on anonymous data and used in research to further the core objectives of The UKCAT Consortium. Given these conditions The UKCAT Consortium does not need to seek the individual consent of candidates to use their data as described in this document.

6. Database Security, Storage and Access

6.1. The UKCAT Consortium has entered into a contract with the University of Dundee Health Informatics Centre (HIC) for the hosting, development and management of its database. Data remain wholly in the ownership of the Board and the Board

retains all rights (including intellectual property) in the data. On the authorisation of the Board, HIC may add data, undertake analysis of the data and publish research findings. HIC Standard Operating Procedures comply with the requirements of the Data Protection Act 1998 and ensure the security of the data. These arrangements are outlined in greater detail in this document. The 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.

6.2. All Data provided to HIC, from PV, medical and dental schools will be via secure encrypted mechanisms, e.g. ftp.

6.3. 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.

6.4. Progression data from medical and dental schools are requested in an excel spreadsheet (candidates are identified by UKCAT and UCAS number only) and provided to the UKCAT office. Data transfers are password protected and passwords for this purpose exchanged by telephone. Data are checked for completeness within the UKCAT Office and then transferred to HIC through a securely. Original data are to be encrypted, archived and stored for a period of five years (to be reviewed) before being deleted. HIC has developed a secure mechanisms to allow The UKCAT Consortium, or medical schools themselves, to upload data directly to HIC..

6.5. All data transfers to the The UKCAT Consortium database are logged in a document maintained by HIC.

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

6.7. 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 UKCAT Consortium would expect the individual to put in place with regard to the storage of the data.

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

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

6.8.2. An open access reporting system to notify of any significant events and an annual external audit of all systems and processes

6.8.3. The HIC Confidentiality and Privacy Advisory Committee (HICCPAC) reviews HIC's methods annually

6.8.4. Routine quality checking, to maintain the accuracy and integrity of datasets

6.8.5. Separate secure access-controlled areas for all data processing and data storage

6.8.6. Nightly offsite mirrored back-up

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

7. Anonymity of Data

7.1. As outlined above, data is received by HIC in an identifiable form. The UKCAT 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 UKCAT 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 The UKCAT Consortium data provided. Published research/analysis will contain aggregate data only.

7.2. The UKCAT 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.

7.3. The UKCAT 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 UKCAT Board.

8. Transfer of Data to Researchers

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

8.2. 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.

8.3. In some circumstances, The UKCAT 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.

9. Data Sharing

9.1. The UKCAT Consortium is working with (amongst others) the Medical Schools Council (MSC) and the General Medical Council (GMC) on creating the UK Medical Education Database (UKMED). UKMED links UKCAT Consortium data, admissions data and University progression data to data held by the GMC and others relating to practising doctors.

9.2. Outputs may include the production of reports on the progression of students and doctors in training and the production of anonymised datasets for use in research.

9.3. The GMC holds The UKCAT Consortium data for the purposes of UKMED under a data sharing agreement. The content of this agreement is referenced at 4.6 above.

9.4. UKMED will facilitate the evaluation of the predictive validity of admission criteria and university performance.

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

10. Data User Responsibilities

10.1. 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 (see **Appendix A**).

10.2. 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.

10.3. When the project is complete the data and the analysis syntax used will be securely archived by HIC.

11. Publication of Findings

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

Rachel Greatrix, Chief Operating Officer, UKCAT

Appendix A: The 8 Data Protection Principles

1. Personal data shall be processed fairly and lawfully
   - 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 obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes
   - Must identify purposes for which data is being processed
   - Must ensure purposes are compatible with information given to data subjects and to the Office of the Information Commissioner (www.ico.gov.uk)
   - Must not further process if purposes are not compatible with consent or notification to OIC without resolving conflicts
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or 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
   - 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 processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
   - 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. Personal data shall be processed in accordance with the rights of data subjects under this Act
   - 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. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

- practical steps to compliance include:
  - do not allow staff to share password
  - site PCs where the screen cannot be seen by unauthorised staff or the public and do not leave information on the screen when you are not there
  - when using external agencies ensure processing is carried out under written contracts
  - block access to systems by former staff
  - vet all prospective employees
  - react to allegations of access to unauthorised data
  - do no leave files unattended in the open
  - shred personal data rather than bin it
  - do not design documents/ write papers in ways that reveal personal data
  - physical and electronic security
  - staff training
  - measures to prevent accidental loss, damage or destruction of data

8. Personal data shall not be transferred to a country or territory outside the European Economic Area (25 EU Member States + Iceland, Lichtenstein & Norway) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

- must not transfer data by any means (including electronic) if in doubt