DATA USE AND RETENTION

Protocol for student and staff research

Reviewed September 2018

ROYAL COLLEGE OF MUSIC London

This document should be read in the context of the RCM's wider Data management (retention) policy.

The protocol described below relates to any research activities undertaken by RCM staff, or students on the doctoral or postgraduate programmes (ie PhD, DMus, MSc, MEd, MMus/MPerf). This document details the issues that should be considered when a new project is being set-up, what details need to be clarified when applying for ethical approval and communicated to participants, and where and how to store data.

The RCM's GDPR policy lists a number of data protection principles that have informed this guidance. Specifically, the data protection principles state that personal data shall be:

- Processed (ie collected, handled, stored, disclosed and destroyed) fairly, lawfully and transparently. As part of this, an organisation must have a 'legal basis' for processing an individual's personal data (eg they have consented to the processing, or the processing is necessary to operate a contract with them, or the processing is necessary to fulfil a legal obligation)
- Processed only for specified, explicit and legitimate purposes
- Adequate, relevant and limited
- Accurate (and rectified if inaccurate)
- Not kept for longer than necessary
- Processed securely

1. Ethics

1.1. All research undertaken at the RCM must be compliant with the CUK Policy on Good Research Conduct. When preparing and submitting your ethics application, state how and where data will be stored and for how long it will be kept. Refer to timelines in table below.

2. Informed consent

2.1. Under the GDPR, an individual's rights (all of which are qualified in different ways) are as below. Each of these points should be made clear within the Information Sheet you provide to participants:

2.1.1. The right to be informed of how their personal data are being used. This right is usually fulfilled by the provision of 'privacy notices' (also known as 'data protection statements' or, especially in the context of websites, 'privacy policies') which set out how an organisation plans to use an individual's personal data, who it will be shared with, ways to complain, and so on. On your Information Sheet, specify how and the purposes for which a participant's data are being used; eg for a research project, PhD thesis, etc.

2.1.2. The right of access to their personal data. Individuals must be allowed to submit subject access requests, which require organisations to provide a copy of any personal data pertaining to them.

2.1.3. The right to have their inaccurate personal data rectified. If the information an organisation holds is inaccurate or incomplete, individuals can request that it be updated.

2.1.4. The right to have their personal data erased (right to be forgotten). In some circumstances, individuals can request that the organisation deletes their personal data. On the Information Sheet you provide to research participants, state that they can request their information be withdrawn and erased but only up until the point at which data analysis begins. After this point, it will be not be possible for a participant to withdraw their research data.

2.1.5. The right to restrict the processing of their personal data pending its verification or correction.

2.1.6. The right to receive copies of their personal data in a machine-readable and commonly-used format (right to data portability).

2.1.7. The right to object: to processing (including profiling) of their data that proceeds under particular legal bases; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest.

2.1.8. The right not to be subject to a decision based solely on automated decision-making using their personal data.

2.2. Other issues that should be clarified on the Information Sheet are:

2.2.1. Who is collecting the data (your organisation or a third party). Typically this should be the lead researcher (student or staff) and any other members of the research team. Such details should be clarified on your Information Sheet;

2.2.2. The legal basis you are using for processing, ie for academic research purposes; and

2.2.3. Whether the data will be shared with third parties. Individual personal data should not be shared, although clarify whether anonymised research data will be shared and with whom and whether the research findings will be disseminated and, if so, how and where.

3. Data storage

Where and how you should store data

3.1. As far as possible, electronic copies of identifiable data pertaining to research participants should only be stored on RCM computers or Office365. Data that is stored on personal devices (ie USB sticks, personal laptops, external hard drives) must be password protected and/or encrypted.

3.2. For staff research, once hard copies of material have been taken to the RCM they should not again be taken out of the RCM and should be locked away when not in use. For student research, hard copies of data should be moved as infrequently as possible and stored in a secure location

3.3. If you need to transfer data, this should be done via Office365 **but not** by Dropbox/Google Docs, etc, as these are not considered secure.

3.4. All identifiable data (i.e. names, contact information, name-code sheets), must be kept separate from datasheets. Documents that link participant information and codes should be password protected, kept in a separate folder from the datasheets, and not be clearly linked to the datasheets. These documents should be deleted as soon as they are no longer required.

3.5. For online surveys (such as those employing SurveyMonkey, etc), if you are giving participants the option of providing their name/contact information so that they can be contacted at a later date, include a statement at the point in the survey when they are requested to provide their name/contact information that their name and data will be stored together for a specified length of time and thereafter stored separately. The length of time that they are stored together should be no more than that during which your survey is live and you are actively collecting data. If using SurveyMonkey, you must turn 'off' the default option that collects participants' IP addresses.

How long should you keep data

3.6. The following are general guidelines for how long data should be kept. As these are general guidelines, specific timeframes should be discussed during the set-up of each new project to make sure they meet the project needs.

Data type	Retention period	Retention Reason
Research source data	No less than 10 years. Project specific.	Transparency/replication/publisher and funder requirements
Ethical approval submissions	No less than 10 years. Project specific.	Kept for as long as data are retained
Research consent forms	No less than 10 years. Project specific.	Kept for as long as data are retained
Master files for randomised control trials (RCTs)	No less than 3 years. Project specific.	Vital interest/member checks/follow on research

3.7. If you think a data breach has occurred (eg because you have lost a laptop, your phone or a USB stick), report the incident to the RCM ICT Helpdesk. They will initiate a first stage investigation and decide if the incident needs to be escalated.

Professor Richard Wistreich
Director of Research