

Cardiff Metropolitan University

Policy on the Storage of Research Data

1. For the purposes of this policy, the term “research data” is clarified as information gathered through the pursuit of research activity. Such information may be in a variety of forms including quantitative data, interview recordings or transcripts, video or audio recordings.
2. Cardiff Metropolitan University acknowledges and endorses the research councils’ statement that *publicly funded research data are a public good, produced in the public interest, which should be made openly available with as few restrictions as possible in a timely and responsible manner that does not harm intellectual property.*
3. Researchers at Cardiff Met are therefore expected to be familiar with and adhere to the Common Principles on Data Policy published by Research Councils UK.
4. Data (including electronic data) must be recorded in a durable and appropriately referenced form. Schools must establish appropriate procedures for the retention of data and for the keeping of records of data held, and must ensure that information about these procedures is communicated to all research staff.
5. Data must be held for sufficient time to allow reference. For data that are published this may be for as long as interest and discussion persists following publication. Data with acknowledged long-term value should be preserved and remain accessible and usable for future research. Conversely, data which has not attracted any interest for more than ten years is not expected to be retained.
6. It is recommended that the minimum period for retention is at least five years from the date of publication. Researchers should however be familiar with any requirements of the funders of their research regarding retention periods and should adhere to these requirements. This being the case, for RCUK funded research, data should be preserved for a minimum of ten years from the date that the researcher’s privileged access period expires or from the last date on which access to the data was requested by a third party, whichever occurs later.
7. Whenever possible, original data must be retained centrally in the School in which they were generated. Individual researchers should be able to hold copies of the data for their own use. However, retention solely by the individual researcher provides little protection to the researcher or the institution in the event of an allegation of falsification of data, and this should be avoided.
8. Data related to publications must be available for discussion with other researchers. To enable this, sufficient metadata should be recorded and made available to enable other researchers to understand the research and re-use potential of the data. Published results should always include information on how to access the supporting

data.

9. Where confidentiality provisions apply (for example, where the researchers or institution have given undertakings to a third party), it is desirable for data to be kept in a way that reference to them by third parties can occur without breaching such confidentiality.
10. Confidentiality agreements to protect intellectual property rights may be agreed between the institution, the researcher and a sponsor of the research. Where such agreements limit free publication and discussion, limitations and restrictions must be explicitly agreed.
11. When the data are obtained from limited access databases, or via a contractual arrangement, written indication of the location of the original data, or key information regarding the database from which it was collected, must be retained by the researcher or research unit.
12. Researchers must be responsible for ensuring appropriate security for any confidential material, including that held in computing systems. Where computing systems are accessible through networks, particular attention to security of confidential data is required. Security and confidentiality must be assured in a way that copes with multiple researchers and the departure of individual researchers.
13. For research where data of a security sensitive nature is acquired and retained, researchers should adhere to Cardiff Met's PREVENT policy which includes the requirement to store this type of data in the central secure storage facility.

RES

December 2014