University policy framework for research data
Utrecht University

1. Structure of this policy framework

This policy framework begins with a definition of research data (section 2). Section 3 looks at the objectives and scope of the framework; specifically, what is this policy framework intended to accomplish and what does fall outside the framework?
Section 4 provides an overview of the current rules and regulations on which the framework is based and also describes the general criteria for effective research data management. Section 5 describes the diverse roles involved in research data management and distinguishes their respective responsibilities. Section 6 establishes the period of validity of the framework.

2. Definitions

Data are recorded facts or circumstances.

Research data constitute
- primary research data: the raw, rough measurements or observations
- Secondary research data: the results after the data have been processed by a researcher (recoded, combined, categorised, visualised, etc.)

External research data: research data made available to Utrecht University and having received, for this use, licensed access to use as a source - but the rights are kept fully outside Utrecht University (such as statistical, financial or survey data).

Archivable research data constitute all research data, excluding external research data, deemed relevant to preserve after the research is completed, for example in connection with the verifiability of the research and/or for possible reuse.

This policy framework applies to all research data.

Research data are intrinsically linked to
- research objects (e.g. geological material, blood samples, archival documents)
- documentation of the research process (e.g. in lab (note-) books)
- *research results*; all inventions, outcomes, materials, methods, processes, products (e.g. publications), programmes, software, findings and/or discoveries generated within the context of a research project

3. Aims and scope

Aim of this policy framework

- Researchers at Utrecht University are supposed to be cognisant of the requirements that the university applies to working with research data. This policy is intended to set parameters to safeguard the quality, availability and accessibility of research data within Utrecht University and also to provide a basis for evaluating compliance with laws, regulations and codes of conduct.
- The policy clearly delineates responsibilities in terms of the roles to be fulfilled by various parties (Executive Board, faculty boards, support and technical staff, research leaders and individual researchers).

Limits

- Faculties/research institutes are in charge of the research objects, for which the policy framework makes no provisions.
- This policy framework does not define a testing procedure.
- The purpose of this policy is **not** to obligate researchers to work with prescribed tools when preserving and releasing research data. The spectrum of UU research is too diverse to impose general guidelines.

4. Basic premises and principles

This policy framework is premised on existing frameworks, which include (but are not limited to):
• the Dutch Personal Data Protection Act
• the Dutch Copyright Act and the Patents Act
• Medical-ethical research protocol requirements pursuant to the Dutch Medical Research (Human Subjects) Act (WMO), as evaluated by the Medical Research Ethics Committee (METC)
• Collective Labour Agreement for Dutch Universities
• Code of Conduct of the Association of Universities in the Netherlands (VSNU)
• Utrecht University's information security policy and ground rules

In addition to the above, Utrecht University applies the following specific principles to data management.

Creation and collection
Research data must be collected, registered, selected and made available for use in accordance with the applicable international standards.

Storage, management and retention
• All research data are to be managed in accordance with the university's requirements governing information security, privacy protection and transparency, in this order of importance.
• Archived research data are to be retained for a minimum of ten years, commencing from the date that the research results are published.
• The data are to be stored safely, protected from unauthorised use and loss.
• The party or parties holding the rights to the data and the parties entitled to use the data are clearly and visibly documented.
• Archived research data are to be stored in a structure that is suitable for long-term preservation and later consultation.
• The full set of research data connected with a research project are to be retained upon its conclusion insofar as relevant for the verifiability of the research.
• The research data will be provided with metadata to describe the data with sufficient clarity to ensure they are findable for further research.
• The retention period and contact details of the data manager are clearly and visibly documented. If research data are to be destroyed, this has to be done in a manner that is verifiable and is irrevocable.

Findability and access
• Digital research should be easy and quick to find.
• Access needs to be furnished in a user-friendly as possible environment in a manner that duly credits and also protects the rights of those who collected or created the data and also protects the rights of those have a legal interest in the manner in which the data are made accessible and used.
• Archived research data are to be made available for access and reuse at and outside Utrecht University insofar as is reasonably possible and subject to the proper precautionary measures. Exclusive rights to reuse or publish research data are not to be transferred to commercial publishers or their representatives without retention of the right to provide open access to the data for the purpose of reuse, except where such transfer is a condition for awarding funds.

5. Roles and responsibilities

Utrecht University distinguishes between the following individual or (groups of) actors, each bearing specific responsibilities for data management.
1. The creators of the data: researchers and students and their supervisors have primary responsibility for data care.
2. Research institute directors are responsible for ensuring that students, researchers and research leaders at their institute abide by the university policy framework and any supplementary faculty regulations. They may also establish further guidelines as needed.
3. Deans draw up additional faculty guidelines pursuant to the university policy framework and are responsible for ensuring that research institute directors implement both the university policy framework and the faculty guidelines.
4. The Executive Board is responsible for the preparation of a general university policy framework, and for monitoring and facilitating its implementation through the provision of infrastructure, information and other forms of support.

A further **general** guiding principle is that each and every staff member must act as a good steward in the management of relevant data.

1. Researchers

It is the responsibility of each individual researcher (or, in the case of a group of researchers, the research leader) to draw up a Data Management Plan (DMP) at the start of the research project and to follow up the agreements made in this plan. The DMP specifies the manner in which research data may be collected, stored, preserved, managed, documented and used. A sample DMP template is available on the Utrecht University intranet.

More specifically,
Researchers are obliged to:
• draw up proper procedures and design processes for the collection, storage, use, reuse, availability and long-term archiving of and provision of access to research data within the research programme. In the case of external data, agreements must be made with the provider of the external data;
• if participating in a joint study or research project to make and record the made agreements on data management;
• ensure that the integrity, confidentiality and protection of the data are guaranteed;
• where the data fall under the Dutch Personal Data Protection Act or under the European Data Protection Guideline, to be aware of their obligations and possible statutory liability;
• make arrangements for the continued operational management of the research data at the end of the research project or termination of their employment contract at the institution;
• factor in the costs for the preservation and management of the research data in research proposals and grant applications.

2. Lecturers and student/PhD supervisors

It is crucial that young researchers (students and PhD candidates) develop an awareness of the importance of good data management and learn about the various options that the institution offers for this purpose. Their supervisors play a key role in developing this awareness. This means that lecturers and those supervising students and PhD candidates are responsible for acquainting their students or PhDs with the university frameworks and disciplinary guidelines governing the collection, storage, preservation, protection and use of data. They must further monitor that students and PhD candidates follow these frameworks and guidelines when conducting their research. It is the joint responsibility of students/PhD candidates and their supervisors to make and record proper agreements on data management and use.

3. Students/PhD candidates

Students are expected to familiarise themselves with the university and faculty policy frameworks and other guidelines applicable to their research and for collecting, storing, preserving, securing and using data in accordance with those frameworks and guidelines.

4. Faculty research institute directors

Faculty research institute directors are responsible for ensuring meticulous research, which also includes conscientious data management. They must ensure that staff and students are aware of their responsibilities and obligations in regard to data management and provide education and training to address any gaps in data management knowledge and skills.

More specifically,
Faculty research institute directors must:
- authorise the procedures that their researchers, students and PhD candidates follow for the collection, storage, use, reuse and (if necessary) deletion of research data;
- ensure that researchers are aware of all their responsibilities and obligations in relation to the research data they collect in the course of their research and that they are sufficiently equipped to fulfil these responsibilities and obligations;
- determine additional guidelines for the storage and long-term preservation of research data at their institute, if desired, which are consistent with guidelines of the faculty, the university policy framework and statutory requirements, and ensure compliance with these additional guidelines.

5. Deans
- Faculty deans are responsible for the implementation and monitoring of the university policy framework and for drawing up additional faculty guidelines to this end if needed;
- Deans are responsible for the meticulous handling and management of data within their respective faculties, in conformity with all statutory and other applicable requirements.

6. The Executive Board
- The Executive Board is responsible for the preparation and adoption of a university policy framework governing research data (in the form of the Utrecht University Research Data Policy);
- The Executive Board is responsible for maintaining and updating the research data policy framework;
- The Executive Board supervises the implementation of the university research data policy framework;
- The Executive Board makes provisions for institutional education, training, support, advisement and, where necessary, the development of guidelines and templates, in any case including a Data Management Plan template;
- The Executive Board ensures that the institution has facilities and services enabling the secure storage of research data for current and future use. This includes storage, backup, registration, repository and long-term preservation services for datasets and the infrastructure needed to provide access to research data and share it with third parties.

2. Period of validity of the policy framework

This policy framework takes effect on 1 January 2016 and is valid until a new version is issued.