

ITC FACULTY OF GEO-INFORMATION SCIENCE  
AND EARTH OBSERVATION


# RESEARCH DATA MANAGEMENT POLICY

WORKING RULES AND GUIDELINES

UNIVERSITY  
OF TWENTE.



## Colophon

ORGANISATION Faculty of Geo-Information Science and Earth Observation (ITC)
DATE Approved by the Faculty Board on 08-04-2024
VERSION Version 1.0
LICENSE This policy is published with a <a href="#">Creative Commons Attribution 4.0</a> International License 
CITE AS The Faculty of Geo-Information Science and Earth Observation, University of Twente (2024). Research Data Management Policy-working rules and guidelines

## Document history

Version	Author(s)	Description
1.0	<a href="#">Alice Nikuze</a> , <a href="#">Masoom Shariat</a>	Original document

## Contents

1. Introduction.....	1
2. Scope of the policy .....	1
3. Definitions .....	2
4. Roles and Responsibilities in Research Data Management .....	2
5. Faculty Guidelines and Working Rules.....	3
5.1 Data Management Planning.....	3
5.2 Data Storage.....	4
5.3 Data Sharing and Transfer .....	4
5.4 Data Documentation.....	5
5.5 Data Preservation .....	6
5.6 Data Registration in PURE .....	7
5.7 Personal, Confidential, and Classified Research Data Management.....	8
References.....	10
Acknowledgment .....	10

# 1. Introduction

The Faculty of Geo-Information Science and Earth Observation (ITC) has committed to promoting open and transparent research practices. Proper Research Data Management (RDM) that is in accordance with FAIR data principles, i.e. ensuring findable, accessible, interoperable, and reusable research data, is a key requirement to achieve this mission. Upholding the best research data management practices is essential for fostering efficient, reproducible, transparent, and high-quality research.

Building upon the solid foundation provided by UT's overarching [Research Data Management Policy](#), the policy outlined below provides **tailored guidelines** and the **best practices** specific to ITC.

This ITC-specific policy is intended to ensure that all research data is handled with the utmost care by all ITC researchers and students in order to, among other things:

- Demonstrate academic integrity, upholding transparency and ethical practices in research;
- Safeguard research data security and the privacy of research subjects;
- Enable research reproducibility, allowing for the verification and validation of academic findings;
- Comply with relevant regulations, policies, and Code of Conduct regarding research data management, including the [General Data Protection Regulation \(GDPR\)](#), [The Netherlands Code of Conduct for Research Integrity](#);
- Ensure the availability of data and facilitate the re-use of research data by the research community.

## 2. Scope of the policy

This policy is intended for all members of ITC engaged in research activities, including master students and academic researchers (PhD candidates, postdoctoral fellows, researchers, and senior academic staff, i.e. assistant professors, associate professors, and full professors) and all other staff involved in the generation, collection, processing, and dissemination of research data. In accordance with UT's RDM policy, it covers roles, responsibilities, and ITC's working rules in accordance with the best RDM practices.

In the subsequent sections, we will delve into specific aspects of RDM, including data management planning, data storage, data sharing and transfer, data documentation, preservation, and registration, and specific considerations regarding handling personal data in research. Each section will provide detailed working rules and information on the best practices for managing research data effectively.

### 3. Definitions

**Research data:** the term ‘research data’ refers to all forms of information, commonly accepted in the academic community, that is collected, observed, generated, or created as necessary to validate research findings and conclusions. Examples include geospatial and remote sensing data, statistics, field and laboratory measurements, experimental and observational data, surveys, interviews, video and audio recordings, photos and images, analysis scripts, etc. (Kruse & Thestrup, 2018). Research data also include secondary documents such as policy reports and data obtained from literature review. Research data do not include the following materials: drafts of academic papers, plans for future research, peer reviews, or communication with colleagues.

**Research project:** In this policy, a research project refers to a detailed study of a subject aimed to solve specific research questions or objectives. It involves the collection, analysis, and interpretation of data in order to discover new facts or develop new concepts, generate new findings, and instigate progress. Research projects explicitly include research carried out by master students and academic researchers (PhD candidates, postdoctoral fellows, researchers and senior academic staff, i.e. assistant professors, associate professors, and full professors).

**Data management plan (DMP):** A DMP is a formal document that describes all data that are to be used in the project, the documentation and organisation of data, data storage during the research process, preservation of data after the project is completed, and finally, the future availability of data for sharing and re-use. The DMP should also provide information on the planned measures to safeguard and protect sensitive data such as personal data (Berez-Kroeker et al., 2022).

**Metadata:** the term ‘metadata’ refers to structured information about data. Such information makes it easier to understand, discover, use, or manage data. It includes information such as the description of said data, their origin, temporal coverage, geographic location, creator, access conditions, and other descriptive elements (Riley, 2017).

**Personal data:** In accordance with GDPR, the term ‘personal data’ refers to any information that relates to an identified or identifiable natural person, such as a name, an identification number, a geographical location, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (European Union, 2016).

**Classified data:** the term ‘classified data’ refers to data that have been classified to a certain level of sensitivity, considering properties such as availability, integrity, and confidentiality, in order to decide the related level of security and protection measures.

### 4. Roles and Responsibilities in Research Data Management

In accordance with UT’s RDM policy, ITC identifies the following individual or (groups of) stakeholders and their responsibilities with regard to RDM:

- **The Faculty Board** is responsible for maintaining good RDM practices as part of the research vision within ITC. Therefore, the Faculty Board is accountable for the implementation of this faculty policy and facilitating that implementation by warranting the availability of infrastructure, tools, and research data management support and expertise, including the presence of a Faculty Data Steward, a Privacy Contact Person, an ICT account manager and an Ethics Committee.



- **Heads of academic departments** are responsible for ensuring that all students in the specializations administered by their departments and all researchers are aware of the Faculty's policy, and for stimulating them to acquire the necessary information and training to manage research data effectively.
- **Academic researchers and students** hold the primary responsibility for taking care of the data that they produce. They must warrant proper data management and adhere to the Faculty's policy.
- **Supervisors/principal researchers and team leaders** are directly responsible for making sure that researchers and students under their supervision are aware of the importance of good data management practices and adhere to the expectations outlined within this faculty policy. More specifically, they must warrant that the research projects under supervision have a DMP in place and that all data underlying the completed research are appropriately documented and preserved as outlined within this policy.

## 5. Faculty Guidelines and Working Rules

### 5.1 Data Management Planning

Planning data management is essential for every research project and should be an integral part of good research design. Quality research starts with a good DMP. Therefore, for every research project conducted within ITC, a DMP must be written and regularly updated during the project.

- **Master students** must write a DMP for their research and include it in the documents required for the proposal. The DMP has to be reviewed by the supervisors as part of the proposal's assessment.
- **PhD candidates** must follow a [Data Management Bootcamp \(1 ECTS\)](#) offered by UT to learn how to write a DMP for their PhD projects. The DMP must be written within the first year of their PhD trajectory, reviewed by the [Faculty Data Steward](#), and included in the documents required for the PhD Qualifier. The DMP for a PhD project must be reviewed annually by the supervisors during the annual interview and updated where necessary.
- **Any other research project** must have a DMP before the start of the said project, but no later than four months after the start of the research, and it must be reviewed by the [Faculty Data Steward](#). The DMP has to be reviewed regularly and updated where necessary and it must be adhered to by all research team members.



A DMP template is available at UT's [DMP-tool](#). The template has been accepted by the Dutch Research Council NWO, the independent governmental body Care Research Netherlands-Medical Sciences ZonMW, and the EU (e.g., the European Research Council ERC). Therefore, the UT DMP template should be used unless the funding body or their partners require the use of a different template.

For support regarding writing a DMP, contact the [Faculty Data Steward](#)

## 5.2 Data Storage

Effective research data management is essential for maintaining the accessibility and security of research data. This section outlines the best practices and guidelines for storing data **during research**. In principle, all research data collected and generated should be stored safely and protected against unauthorised access, accidental disclosure, and loss. The choice of storage facility depends on many factors, such as the type of data, size, the need for collaboration with research partners, etc.

- **A copy of key research data** (key files of the data collected and generated) and the related materials (e.g. documentation, protocols, models, or questionnaires) **must be stored in facilities offered by UT**, unless exceptions apply.
- **In case researchers wish to use their own storage facilities for primary storage**, note that UT has strict requirements when it comes to acquisition of research data storage. **It is required to ensure that the storage facility is at least [ISO 27001](#)-certified and in the case of health data [NEN 7510](#)-certified**. These two certificates prove that the way data, especially personal and privacy-sensitive data, are stored complies with current security standards. If you need advice regarding the storage certification, please contact the [Faculty ICT Account Manager](#)
- **Portable devices** (e.g., external hard drives, USB sticks, or personal laptops) **should not be used as the primary storage facility of research data**.
- **Non-digital research data** and related materials, such as physical samples, lab notebooks and printed informed consent forms, **must be stored in accordance with clearly described procedures and standards within the research group** and/or project and must be digitised where possible.



Take a look at the [UT storage decision tree](#) which provides an up-to-date overview of UT storage facilities and all other secure storage solutions offered by UT.

Contact the [Faculty Data Steward](#) in case you have questions or need support.

## 5.3 Data Sharing and Transfer

Data sharing refers to providing access to data in a way that maintains the data's availability, accessibility, and confidentiality. This section outlines the best practices and guidelines for data sharing with colleagues within or outside ITC **during research**.

- Stored research data should be **accessible to at least one other member of the research team other than the main researcher**, ideally the principal researcher or a daily supervisor for Postdocs, PhDs, and Master students. Access to the stored data by other research team members is vital to ensure data availability.
- For collaborative projects involving data sharing, a **data sharing agreement**, which establishes the terms and conditions under which data are shared and clarifies the roles and responsibilities of both parties regarding the management of the data, should be

drawn up in consultation with the [Faculty Privacy Contact Person](#) and **should be signed by the Faculty Dean prior to sharing research data with external parties.**



- The [UT storage decision tree](#) also offers a range of facilities for data transfer and data sharing.
- **There are several types of data sharing agreements**, depending on the research project and type of data:
  - **A data transfer agreement** is generally used when sharing **non-personal data** with third parties;
  - **A joint controllership agreement** is used to establish shared responsibilities regarding the processing of **personal data** with collaborators. Consortium agreements and Grant Agreements (e.g., Horizon 2020) provide a legal basis for this type of agreement;
  - **A data processing agreement** is used when a third party is involved in the processing of **personal data** on behalf of the data controller (such as collecting, storing, or analysing the data on your behalf);
  - **A non-disclosure agreement** is typically used for trade or commercial data, including trade secrets and patent-related data.

## 5.4 Data Documentation

Data documentation is crucial to ensure that research data are understandable and re-usable by yourself or by others. In accordance with the FAIR principles, as a minimum requirement a definite version of research data should be well documented. However, best practice is to start documenting data and record metadata early during the research process and to update these regularly throughout research in order to warrant completeness and accuracy.

- Research data, both digital and non-digital, should always be accompanied by metadata to ensure findability and re-usability.
- Research data must be accompanied by additional documentation (e.g., in the form of a README file, data paper, etc.) to enable correct interpretation and re-use. Clear, concise language and standard terminologies should be used to ensure comprehensibility.





- Research data must be accompanied by at least one set of metadata for the entire dataset. However, for comprehensive documentation, metadata should be provided for each distinct type of data or file where applicable or necessary.
- Since the data repositories provide machine-readable forms of metadata, most often based on a generic metadata standard such as [Dublin Core](#), it is recommended to provide additional documentation in the form of a README file. This documentation should encompass, but not be limited to the data contents and structure, along with all relevant methodological information (e.g., the collection, processing, and quality control aspects of said data), records of different versions of the data files, and details on sharing and access.
- Discipline-specific metadata standards (e.g., the [ISO 19115 geographic information metadata standard](#)) can be used to decide on additional information aimed at enhancing the data documentation.
- For the local management of your research datasets and related metadata and for publishing them easily to different research data repositories, you can use the [fairly toolset](#). This toolset includes a command line tool and a JupyterLab extension that facilitate creating, uploading, and downloading research datasets together with metadata without requiring programming skills.

## 5.5 Data Preservation

Data preservation refers to the long-time storage of research data to enable the verification and reproduction of research and the re-use of data. Publishing and archiving data are the two most practical ways to preserve data after research.

- **Digital research data** needed for verification and reproduction (at least those underlying all types of academic publications, such as journal articles, reports, theses, etc.) **have to be preserved** in one of ITC's approved data repositories or archive facilities for **at least ten years** after completion of the project (in accordance with [The Netherlands Code of Conduct for Academic Practice](#)).
- **Preserved in a repository**, research data can be published **publicly, with restricted access, or embargoed**. In accordance with the [ITC's Open Science Strategic Plan](#), the data should be published as open as possible and as closed as necessary, i.e., in case of legitimate reasons, such as ethical reasons, reasons concerning privacy protection and national security reasons, [knowledge safety and export control](#), confidentiality, commercial interest, legal and contractual obligations reasons. However, the **metadata must always be made available publicly**.
- Digital **research data that cannot be shared with third parties**, including trusted data repositories, **must be archived in UT's archive facility**.
- Research data underlying **master's and PhD research projects** must be preserved **before graduation**. Research data underlying **other types of research projects** must be preserved **no later than one month** after completion of the research project.

- **Non-digital research data**, wherever possible and appropriate, should be digitised. If the data is to be preserved in non-digital format, they should be stored securely in accordance with the respective department's common practices.
- **The primary author and co-authors** of academic publications share the responsibility of **controlling access** and making any decision with respect to the data and, therefore, should all be acknowledged in the metadata of the archived or published datasets as contact persons.
- For research projects run by ITC researchers, **access to the data with restricted access is controlled by the principal investigator**. In situations where the original researchers are not available or no longer affiliated with ITC, access to the data is determined and granted by the **department chair**.
- Archived or published digital and non-digital research data require sufficient documentation to enable proper interpretation and re-use, as described in the section on Data Documentation.



- For publishing research data, UT and ITC recommend two trusted research data repositories: [DANS](#) and [4TU.ResearchData](#).

Trusted repositories are the repositories that have received a [Core Trust Seal Certification](#), which warrants the reliability and durability of data repositories and, hence, the potential for storing data over a long period of time.

- For archiving research data, UT has a certified facility for long-term research data archiving known as [AREDA](#). It is required to contact the [Faculty Data Steward](#) before archiving data in AREDA.
- For archiving research data from master research projects, ITC has a separate archive facility.

## 5.6 Data Registration in PURE

The registration of research output in Pure, including **research data**, is essential for consolidating information from various sources at one single platform in order to offer a comprehensive overview of ITC research activities and their impact.

- All archived or published digital and non-digital data **must be registered in** [Pure \(UT Research Information\)](#), where their metadata information is recorded to increase visibility.



Step-by-step guidelines, including a Demo and more guidance on registering research output, are available on the [UT Research Information Website](#)

## 5.7 Personal, Confidential, and Classified Research Data Management

Warranting the protection of confidential data, privacy, and the rights of research subjects is paramount in all research activities conducted within ITC. This section outlines key principles, practices, and compliance measures related to the handling of personal and confidential data in research:

- All research activities involving personal data must adhere to the principles and requirements outlined in the GDPR;
- Researchers should only collect the **minimum amount of personal data** necessary for research purposes. Collecting unnecessary or excessive personal data should be avoided;
- Researchers and students must report any processing of personal data through **GDPR registration** using the online UT [DMP+GDPR tool](#);
- A **Data Protection Impact Assessment (DPIA)**, i.e, **risk assessment**, should be carried out prior to processing any personal data likely to result in high risks to the rights and freedom of data subjects;
- Personal data, confidential and classified data must be protected against unauthorised access and loss as much as possible. More particularly, personal data should be stored in a **GDPR-compliant data storage facility** and, where needed, additional security measures such as encryption should be applied;
- **Personal data should be anonymised or pseudonymised** as soon as possible, preferably immediately after collecting those data. Similarly, secondary datasets containing personal data should be pseudonymised or anonymised immediately after receiving them. Note that unlike anonymised data, pseudonymised data are still personal data;
- Prior to sharing research data containing **personal data**, a **data processing agreement** should be drawn up in consultation with the Faculty Privacy Contact Person and should be signed by the Faculty Dean. A **non-disclosure agreement** is required in the case of sharing **confidential and classified data**; see more details under the “Data Sharing and Transferring” section in this policy;
- Personal data needed for verification and reproduction (at least those underlying all types of academic publications, such as journal articles, reports, theses, etc.) **have to be preserved** in one of ITC’s approved data repositories or archive facilities for **at least ten years** after completion of the project (in accordance with [The Netherlands Code of Conduct for Academic Practice](#));
- **Informed consent forms** used to collect personal data, either in digital or non-digital form, **have to be archived for at least ten years** after completion of the research project;
- Researchers **must report any [data breaches](#) immediately**. Examples of potential data breach include devices containing personal, confidential and classified data being lost or stolen, sharing these data with the unauthorised persons, etc. For more information on data breach, see [Cyber Safety at UT](#);
- Research involving human subjects or potentially sensitive data about or from individuals, groups or organisations **must be reviewed** by the [ITC Ethics Committee](#) before the work commences. For other types of research, it is strongly recommended to identify potential ethical issues related to, for instance, the environment, dual-use aspects, low-income countries, or artificial intelligence, through an ethics review.



- More information on the appropriate use of personal data in research, including a flowchart and practical guidance, can be found on the [UT Cyber Safety Website](#).
- This [pre-DPIA assessment](#) form should be used to find out whether a full DPIA is required.
- **UT network storage facilities** (e.g., P-drive, Unishare,) are ISO 27001-certified, NEN 7510-certified and GDPR-compliant; therefore, they guarantee maximum security **for storing and sharing** personal data, confidential and classified data during research.
- For personal data stored in **non-UT cloud storage** (e.g., MS Teams, OneDrive, etc.) or on **portable devices** (e.g., USB sticks, external hard drives, tablets, etc.), **encryption is required**.
- Personal data stored **on portable devices must be deleted as soon as possible** and no later than at the end of the part of research for which the data are needed (e.g., after fieldwork).
- **The encryption key** must be kept safe and stored in a separate location. Furthermore, it should be shared with at least one other employee in the research group. Generally, this person will be the principal researcher or the chair of the research group.
- **Non-digital informed consent forms** should be digitised where possible. However, UT has an archive service for **non-digital informed consent forms**. Please contact the [Faculty Data Steward](#) for support.
- To submit your application for ethics review, visit the [ITC Ethics Committee website](#) or contact the Faculty's [Research Support Officer](#).

For support regarding the handling of personal data in research contact the [Faculty's Privacy Contact Person \(PCP\)](#).

## References

- Berez-Kroeker, A. L., McDonnell, B., Koller, E., & Collister, L. B. (2022). The Open Handbook of Linguistic Data Management. In A. L. Berez-Kroeker, B. McDonnell, E. Koller, & L. B. Collister (Eds.), *The Open Handbook of Linguistic Data Management*. The MIT Press. <https://doi.org/10.7551/mitpress/12200.001.0001>
- European Union. (2016). *General Data Protection Regulation (GDPR)* (Issue 27 April). <https://autoriteitpersoonsgegevens.nl/uploads/imported/gdpr.pdf>
- Kruse, F., & Thestrup, J. B. (2018). *Research Data Management – A European Perspective* (F. Kruse & J. B. Thestrup (eds.)). Walter de Gruyter GmbH. <http://site.ebrary.com/lib/staffordshire/docDetail.action?docID=10521727&ppg=1>
- Riley, J. (2017). *Understanding Metadata*. National Information Standards Organisation (NISO). <https://groups.niso.org/higherlogic/ws/public/download/17446/UnderstandingMetadata.pdf>

## Acknowledgment

Input and feedback on this policy have been provided by all Department Research Portfolio Holders. Contributions in the form of reviewing and editing have been made by:

- Prof. Dr. Karin Pfeffer - Portfolio holder research
- Dr. Ir. Jelle - Research coordinator
- Dr. Ing Serkan - Center of Expertise in Big Geodata Science (CRIB)
- Prof. Dr. Justine Blanford - Program director for the Master's in Geo-Information and Earth Observation Sciences (MGEO)
- Drs. Jeroen Verplenke - Programme manager/Internationalization coordinator
- Project officers and managers (all)
- Annika van der Putten - UT Privacy officer
- Drs. Petra Buddle - Remote sensing and GIS Lab
- Prof. Dr. Mark van der Meijde – Head of the Applied Earth Sciences department

We acknowledge and thank all the above contributors for their input and feedback, which helped to shape the policy to its current state.