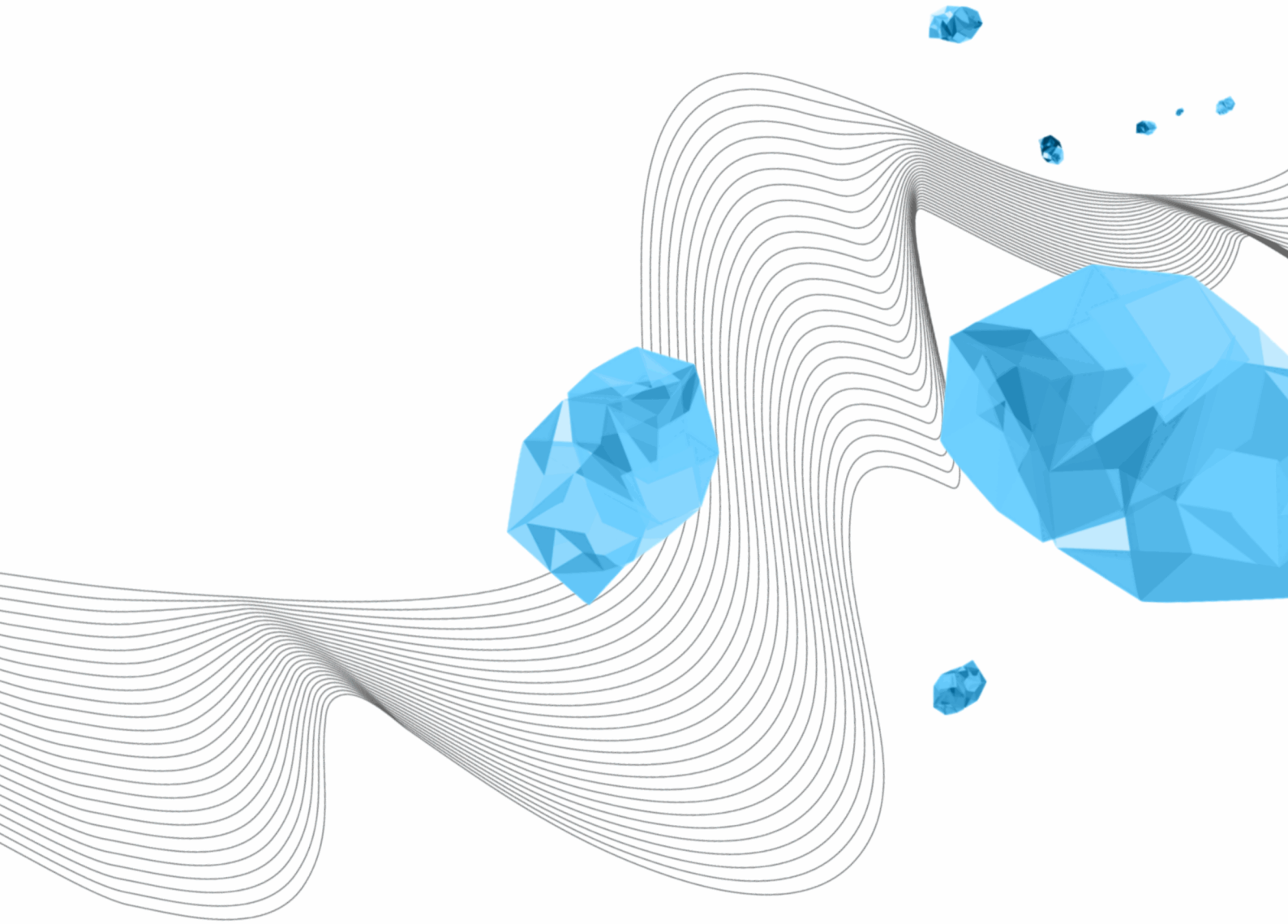
RESEARCH DATA MANAGEMENT POLICY FACULTY OF ENGINEERING TECHNOLOGY

Reference: ET.23.19925
Version: 1.2
Confirmed by the Faculty Board of the faculty of Engineering Technology on 05-05-2023



UNIVERSITY OF TWENTE.

TABLE OF CONTENTS

1 Introduction 3
2 Faculty-specific roles and responsibilities 3
3 Data management plan (DMP) 3
4 Privacy regulations 3
5 Data storage and transfer 4
6 Data documentation 5
7 Data sharing 5
8 Data archiving 6
9 Data registration 7
Appendix A Faculty-specific roles and responsibilities 8
Appendix B FAIR principles 9
Appendix C List of abbreviations 10
Appendix D Archiving Paper informed consent forms 11

Document management:

Version	Author(s)	Description
1.0	Maria Kamp	Original version
1.1	Maria Kamp, Simone Fricke	Updated based on latest developments at the UT/ET (e.g. decision tool for data storage, archiving informed consent forms), small textual changes
1.1.1	Victor Wanningen	Updated email address in Appendix E Archiving Paper Informed Consent Forms
1.2	Maria Kamp, Victor Wanningen	Updated based on the latest RDM developments at the UT/ET.

1 INTRODUCTION

The information in this policy applies to all professionals who conduct and support research within the faculty of Engineering Technology (ET). It concerns all activities that are part of conducting research, like generating, processing, interpreting, archiving, publishing, sharing and or distributing or deleting research data. This policy aims at offering guidance and making concrete what is needed for ET research to achieve the main goal of good data management and is based on the UT Research Data management (RDM) policy that is confirmed by the Executive Board of the UT on 17 September 2018. All working rules mentioned in this policy are supplementary to the general UT policy and should be read and handled as such.

This policy is intended to ensure the careful handling of research data by researchers in order to:

- Demonstrate the scientific integrity of their research.
- Stimulate reuse of the data.
- Comply with legal requirements, codes of conduct and funding bodies' demands regarding research data management.
- Offer a framework for data agreements and handling in case of the involvement of third parties.

For questions about this ET RDM policy document and/or if you need advice on RDM, the ET Faculty Research Data Steward is your first point of contact.

2 FACULTY-SPECIFIC ROLES AND RESPONSIBILITIES

The roles and responsibilities are described in Appendix A Faculty-specific roles and responsibilities.

3 DATA MANAGEMENT PLAN (DMP)

The general UT RDM policy states that every research project must have a DMP. For every research project, including each PhD-project a DMP should be formulated. Note that most research funders also require a DMP as part of funding application or to be handed in shortly after the start of the project.

DATA MANAGEMENT PLAN | ET WORKING RULE

For every research project, including each PhD-project, a DMP should be formulated and used during the duration and finalization of the project. For research projects where no PhD-students are involved, a DMP has to be in place as soon as possible but not later than 2 months after the start of the project. A template is available in the DMP-tool of the UT. This template is accepted by NWO, ZonMW and the EU (e.g. ERC).
Every PhD candidate develops a written DMP for managing research outputs within the first 9 months of the PhD and follows the Data Management Bootcamp (1 ECTS) as a preparation of writing the DMP. Each PhD candidate adds the DMP to the documents required for the Qualifier.
The RDM policy of the group or department and the DMPs (pdf export from the UT DMP-tool) are stored directly accessible to the head of the research group and individual researchers and must be stored in the groups folder on the Project and Organization directory (P-drive), or on UT SharePoint or Microsoft SharePoint/Teams.

4 PRIVACY REGULATIONS

ET research groups may handle **personal data**; any data about an identified or identifiable person. A name, birthdate, address, real ID-number or photograph can identify someone. Anonymization of personal data means de-identification that is not reversible: once personal data has been stripped of identifying data, it is no longer possible to trace back to natural persons. Pseudonymization means that personal data are replaced by a key, making it possible to trace back to natural persons.

DATA PRIVACY REGULATIONS | ET WORKING RULE

Personal data are handled according to UT privacy rules. Informed consent forms should be used for research with human participants, and the General Data Protection Regulation (GDPR) should be followed. Report any new processing which uses personal data to the Data Protection Officers (DPO) team. This can be done using the GDPR registration function in the UT DMP-tool. The Privacy Contact Person (PCP) of the ET Faculty is able to support you. Only anonymized data is exempt from the GDPR registration since it is by law no longer personal data.
The processing of personal data in research must be proportionate to the intended purpose of the research. This means that personal data must be limited to what is necessary in relation to the purposes for which they are processed ('data minimization' principle). In other words, don't process personal data if it is not necessary for the research project.
Research data should not include identifiers which directly identify persons (such as name, birthdate or real ID-numbers). During the research, personal data must be anonymized or pseudonymized as quickly as possible, i.e. immediately when collecting data. If you receive a data set with identifying data from another party, pseudonymize or anonymize immediately after receiving the data. The basic steps of pseudonymization can be found on the website of LCRDM. Any exceptions, such as for video footage of people, are described in the group/department policy or DMP.
Research which involves interaction with, or data gathered from, human subjects is submitted by the researcher to a domain specific ethics committee(-member) for an ethical review by means of the Ethical Review tool. Moreover, research is subject to the WMO (Wet medisch-wetenschappelijk onderzoek met mensen) if it concerns medical-scientific research and if the participants are subject to procedures or are required to follow rules of behavior. In case that it is not clear whether a research project is subject to the WMO or not, the details must be reviewed by an employee with knowledge of the WMO before submitting a medical ethical review of the research project.
For research which involves interaction with human subjects, personal data must be managed in a GDPR compliant ICT system suitable for personal data, such as the UT P-drive, or accessible to UT researchers through the ICT system(s) of the involved medical partner institution(s). For the UT P-drive, it is possible to set access rights at folder level by LISA, or the ICT contact person within the department.
Paper informed consent forms need to be kept and archived. An option that is offered by the ET Faculty (archived at the UT) is described in Appendix D Archiving Paper informed consent forms.

5 DATA STORAGE AND TRANSFER

Data storage concern all storage during the research. After a research project the term data archiving applies, which is described in Data archiving. During the research data should be stored in such a way to minimize risk of data loss and to maintain data integrity. Research groups should also take security measures to avoid loss of research data during the course of a research project, due to e.g., theft of laptops, fire and water damage, or a sudden leave of a researcher without the group having access to the data.

DATA STORAGE | ET WORKING RULE

All collected research data, including related materials (e.g. protocols, models or questionnaires), must be stored in an ISO 27001- and NEN 7510-certified directory such as the Project and Organization directory (P-drive) including backups hosted by or offered through LISA, unless exceptions apply. Exceptions must be described within the department policy to comply with the principles of the ET Faculty policy and must always be coordinated with the ICT account manager of the ET Faculty. All research data should be accessible by at least one permanent staff member of the research group besides the principal investigator. All storage solutions offered/recommended by the UT are shown in the UT Storage-Decision-Tree tool.
If storage for group use is not an option and private / personal storage is needed for research data, it must be ISO 27001-certified and accessible to the head of the research group or delegate. Data on personal storage are moved to group storage (in the ISO 27001- and NEN 7510-certified Project and Organization directory (P-drive)) in case the researcher is no longer employed at the research group no later than 1 month before the end of the contract.
Personal cloud services must only be used for work copies, comply with legal and contractual conditions, and be accessible to the head of the research group or delegate. The preferred personal/private cloud service is Surfdrive in which folders should be shared with the head of the research group or delegate and can be synchronized with local storage. This service complies to the Dutch and European privacy legislation. The original data must be stored in the Project and organization directory (P-drive).
Personal, confidential or classified research data and related materials, such as consent forms, will be stored in accordance with relevant Dutch legislation and European regulation and the VSNU Conduct code for the use of personal data in scientific research, for which UT-storage mentioned above is available (e.g. P-drive). Loss of personal or confidential data must be considered as a data breach. To avoid a data breach always use data encryption. For more information see: Cyber Safety.

The use of portable storage should be minimized. In case of portable storage (USB-sticks, external hard drives (HDD), laptops etc.) data is stored as short-term as possible, is encrypted, and is backed-up regularly on non-portable storage accessible to the head of the research group or delegate. Confidential research data on portable devices must be deleted as soon as possible and no later than ending the research task for which the data is needed.
In case of portable devices AND confidential/personal data (as a rule pseudonymized): data **must** be encrypted. In case of data encryption, the encryption key should be known by at least one other employee in the research group. Generally speaking, this will be the direct supervisor. More information about data encryption can be found here.
Non-digital research data and related materials (all data which are the basis of published results), such a physical samples and lab notebooks, are handled according to procedures described in a department RDM policy or DMP. Digitalization is done if (technically) possible.

6 DATA DOCUMENTATION

Data documentation is 'information about the research data'. In line with the FAIR principles (Appendix B FAIR principles) data must be well documented, during the dynamic phase of the data and especially as soon as they have become static. Metadata is 'data about data'. It is standardized, structured information that describes the purpose, origin, time frame, geographic location, creator, access conditions and terms of use of a data set.

DATA DOCUMENTATION | ET WORKING RULE

Research data will be provided with metadata to ensure findability and unique identification of the data; see the metadata guidelines of 4TU.ResearchData. Additional documentation must accompany the data required for correct interpretation and reuse of the data set. Besides the contextual project information, the data documentation should also include how the research data was generated, processed, and stored, such that others from the same research field can understand and work with the data. Typically this is achieved by means of adding README file(s); see the README file guidelines of 4TU.ResearchData. Metadata and data documentation must be stored in a separate file in the concerned directory and must be in place before publications or reports are published. For all publications and reports a record is kept on which data it is based. These links are mentioned in the publications or stored separately with the project documentation.
The data documentation should also describe which software, including version number, has been used. Self-written software/code (e.g. Python, Matlab, Labview) should contain sufficient documentation so that others (from the same research field) are able to understand and (if possible) re-use it.

7 DATA SHARING

Data sharing focuses on sharing during the research. To guarantee that data can be accessed and checked during the research, digital and non-digital research data and related materials must be shared. Implementation is dependent on intellectual property and responsibilities regarding research data, and the terms of use of data suppliers.

DATA SHARING | ET WORKING RULE

During the research project, data and related materials must be shared in such a way that, apart from the researcher, it can be accessed by at least one permanent staff member of the research group. At the end of the project all research data and related materials which is needed for verification/replication and reuse, must be made available to the head of the research group or delegate.
Personal, confidential or classified research data and related materials, such as consent forms, must be shared in accordance with relevant Dutch legislation and European regulation and the VSNU Conduct code for the use of personal data in scientific research (VSNU Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek). The ISO 27001- and NEN 7510-certified Project- and Organization directory (e.g. P-drive) of the UT must be used for secure sharing of personal data. For project members who are not UT employees, this can be arranged through an X-account. LISA can arrange this. Alternatively, Surfdrive, UT SharePoint, and Microsoft SharePoint/Teams, provided the UT credentials are used to login, can also be used for sharing and collaborating on research data with both UT and non-UT (external) researchers.

In case of a Non-Disclosure Agreement, Data Transfer Agreement, or Consortium Agreement with third parties, arrangements must be made about sharing data during the research. Data are shared / exchanged with external partners (non-UT) according to a signed agreement between parties regarding their research cooperation. In addition, Confidentiality and Intellectual Property Right Assignment Agreements with Bachelor and Master students need to be drawn up as well to properly manage intellectual property rights (IPR) for research projects. For the ET Faculty, signed agreements are drawn up by the ET Project Calculations Office.

8 DATA ARCHIVING

Data archiving concerns with data preservation and if possible making data publicly available after (ideally towards the end of) a research project for the purpose of verification, replication and if possible reuse. In the light of Open Science and scientific integrity, sustainably archiving of static data and providing access is crucial. At the end of each research project, the research data, metadata, and additional data documentation should be archived at the UT, and if possible in a sustainably administered trusted public repository, such as 4TU.ResearchData. At a minimum, archiving applies to all data used for and/or underpinning scientific publications, including dissertations, that cannot in its entirety be found in the publication itself or in the 'supplementary information' accompanying the publication. Archiving also refers to both experimental data and numerical models, for which entry files and result files can be archived. Scientific publications that are highly theoretical may already contain all data required for verification and reuse.

DATA ARCHIVING | ET WORKING RULE

Selected research data (at minimum all data which are the basis of published results) and related materials must be archived at least for 10 years (requirement of the 'Nederlandse Gedragscode Wetenschapsbeoefening' and the UT RDM Policy), unless legal or contractual regulations demand another term.
Not later than 1 month after publishing, the selected research data (at minimum all data which are the basis of published results), including a filled out metadata sheet and proper data documentation by means of Readme files, should be archived in the research group's storage facilities, such as the P-drive, UT SharePoint, or Microsoft SharePoint/Teams. If it concerns sensitive research data, e.g., personal data and/or data with commercial interest, additional safety measures must be taken. For instance, access control on the P-drive (available through the self-service portal of LISA), on UT SharePoint, and on Microsoft SharePoint/Teams, and data encryption. Note that the data encryption keys need to be securely managed by at least one permanent staff member of the research group besides the principal investigator, preferably the chair of the research group.
As one of the first universities in the Netherlands the UT has launched the first version of its Archive REsearch DAta (Areda), a UT-wide facility to preserve research data for at least 10 years. Besides the research group's storage facilities, research groups can make use of Areda, provided research data per project is smaller than 1TB, doesn't contain personal data (only pseudonymized and/or fully anonymized data), and commercially sensitive data is encrypted. Note that the data encryption keys need to be securely managed by at least one permanent staff member of the research group besides the principal investigator, preferably the chair of the research group. So, Areda can be used in accord with its current instructions. The research data uploaded to Areda is closed as it will only become available to the research group conform the HR structure. The associated metadata and data documentation are registered in the UT Pure system, which will become publicly available. Over the course of 2023 and beyond, the Areda system will be upgraded to accommodate more complex archiving requests and will have additional procedures and functionalities. It is required to contact the ET Faculty data steward on how to use Areda and to inquire about its latest developments.
Digital informed consent forms and pseudonymization key files for the pseudonymization process of personal data need to be encrypted and archived separately from the archived research data on separate servers, also for the duration of at least 10 years.
Non-digital research data and related materials, such as physical samples or lab notebooks, must be archived in secure UT-storage options accompanied with clearly described access procedures.
Archived research data and related materials, both digital and non-digital, are accompanied with proper metadata for findability and good data documentation for reasons of interpretation and reusability (see also data documentation and data registration).
Within the context of the transition to Open Science, funders increasingly require data to be publicly available, i.e., research data to be open. Unless there are legal or contractual restrictions, data could also be made openly available in a trusted repository such as 4TU.ResearchData or DANS, in accordance with the FAIR data principles (Appendix B FAIR principles). If it is not allowed to make the data openly available (e.g. due to collaborations with companies), if possible,

data could still be made available in a trusted repository with restricted access or an embargo. Otherwise long-term storage at the UT could be a viable option. Unless fully anonymized, it is not allowed conform the GDPR to upload personal data to public repositories, but to use an UT archive instead. Once data sets, including proper metadata and data documentation, are uploaded to for instance 4TU.ResearchData, they get a DOI and become citable in for instance research papers. 4TU members, like UT employees, can upload 1TB per year free of charge to 4TU.ResearchData.
In case of a Non-Disclosure Agreement, Data Transfer Agreement, or Consortium Agreement with third parties, arrangements must be made about archiving and sharing of data for verification and replication. For the ET Faculty, signed agreements are drawn up by the ET Project Calculations Office.
Research groups are responsible for making their research data available for third parties, considering the legal and contractual demands with respect to publicity and privacy. This holds for data which is made publicly available on forehand, or for data made available on request. Also recent developments and guidelines on knowledge safety, and the UT policy on knowledge safety & export control need to be taken into account before sharing and/or making data publicly available. In the context of Open Science, the intentions should be to make data sets publicly available, where appropriate.

9 DATA REGISTRATION

In addition to archiving, all digital and/or non-digital research data and related materials must be registered and described by metadata, including a link or reference to the location of the digital or non-digital objects. Because research data is becoming a valuable asset and data can also be considered as a type of scientific output, it is important to know which digital and/or non-digital research data and related materials have been created or used and where these are stored.

DATA REGISTRATION | ET WORKING RULE

The preferred system for registration of metadata of digital and/or non-digital research data and related materials is the UT Research Information System (Pure portal) which allows for relatively short and structured registration of datasets. By describing datasets and their location in Pure, the metadata and data documentation can easily be found by other researchers in UT Research Information System (Pure portal) and as such in search engines like Google Scholar. In Pure the metadata and data documentation for your datasets can be registered and, via a DOI, linked to the actual dataset which you have archived in a trusted public data repository. Or you can suffice with describing the dataset with metadata and data documentation and where it is located (e.g., Areda), if it concerns material that cannot be uploaded to a trusted public data repository. Moreover, in Pure these datasets and related materials can be linked to the registered UT projects and to UT publications based on them.

APPENDIX A FACULTY-SPECIFIC ROLES AND RESPONSIBILITIES

The roles and responsibilities for different stakeholders within the faculty ET are defined in this policy and described below.

THE FACULTY BOARD

• Is responsible for this policy and the implementation. In particular the portfolio holder research is assigned for this task.
• Ensures that the faculty policy is reviewed annually.
• Oversees the creation of the department data policies.
• Arranges RDM support and expertise in the faculty: ICT account manager, Information specialist, privacy contact person, coordinator research support, research data steward, and ethics committee.
• In case a research group is dissolved, the Dean of the ET Faculty has the authority to grant access to research data.

THE HEAD OF THE RESEARCH CHAIR

• Is partly responsible for having RDM regulations and procedures on the level of his or her department and makes sure that everyone within the group knows about the department data policy.
• Is responsible for proper data management within all research projects performed within the group.
• Is responsible for the correct selection and persistent availability of data of all projects of the research group for the purpose of verification/replication and reuse.
• Arranges the availability of the necessary resources, facilities and support for data management in the research group.

RESEARCHER

• Is responsible for the way he/she deals with research data, in some cases together with the principal investigator and develops and adopts appropriate procedures and processes for collecting, documenting, storing, processing, using, accessing and sharing of the collected or generated research data and for selecting and archiving the research data.
• Ensures that every research project starts with a data management plan (https://webapps.utwente.nl/dmp), which needs to be regularly updated and adhered to by all project members.

APPENDIX B FAIR PRINCIPLES

Preamble

One of the grand challenges of data-intensive science is to facilitate knowledge discovery by assisting humans and machines in their discovery of, access to, integration and analysis of, task-appropriate scientific data and their associated algorithms and workflows. Here, we describe **FAIR** - a set of guiding principles to make data **Findable, Accessible, Interoperable, and Re-usable**.

To be Findable:
F1. (meta)data are assigned a globally unique and eternally persistent identifier.
F2. data are described with rich metadata.
F3. (meta)data are registered or indexed in a searchable resource.
F4. metadata specify the data identifier.

To be Accessible:
A1 (meta)data are retrievable by their identifier using a standardized communications protocol.
A1.1 the protocol is open, free, and universally implementable.
A1.2 the protocol allows for an authentication and authorization procedure, where necessary.
A2 metadata are accessible, even when the data are no longer available.

To be Interoperable:
I1. (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.
I2. (meta)data use vocabularies that follow FAIR principles.
I3. (meta)data include qualified references to other (meta)data.

To be Re-usable:
R1. meta(data) have a plurality of accurate and relevant attributes.
R1.1. (meta)data are released with a clear and accessible data usage license.
R1.2. (meta)data are associated with their provenance.
R1.3. (meta)data meet domain-relevant community standards.

Source and further information: https://www.force11.org/group/fairgroup/fairprinciples

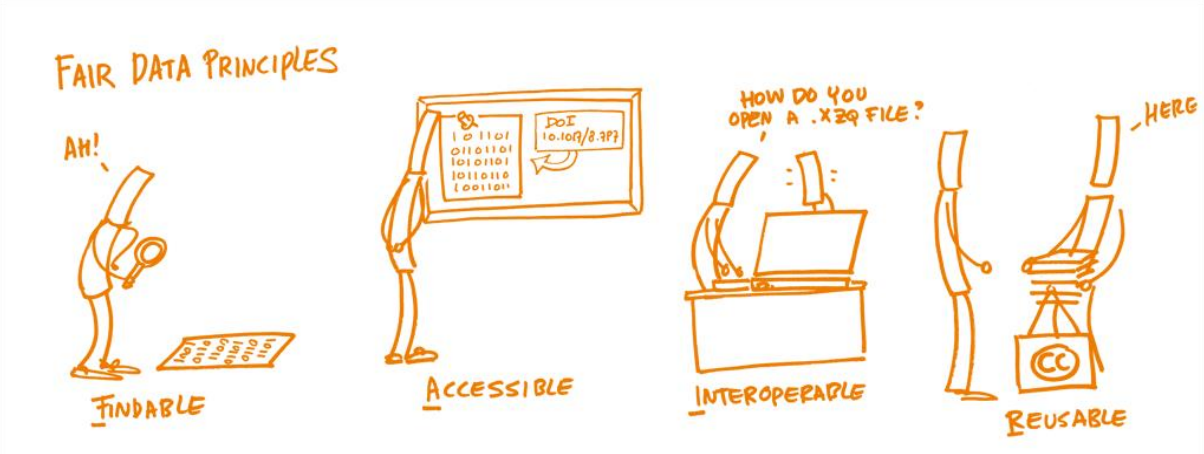


Figure 1 - Fair Data Principles (source: Open Science Training Handbook)

APPENDIX C LIST OF ABBREVIATIONS

DMP	Data Management Plan
DOI	Digital Object Identifier
DPO	Data Protection Officers
ERC	European Research Council
ET	Faculty of Engineering Technology
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Re-usable
GDPR	General Data Protection Regulation
LCRDM	Landelijk Coördinatiepunt Research Data Management
LISA	Library, ICT-services & Archive
M-drive	Home directory
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
PCP	Privacy Contact Person
P-drive	Project and Organization directory
RDM	Research Data Management
TGS	Twente Graduate School
UT	University of Twente
VSNU	The Association of Universities in the Netherlands
WMO	Wet medisch-wetenschappelijk onderzoek met mensen
ZonMW	The Netherlands Organisation for Health Research and Development

APPENDIX D ARCHIVING PAPER INFORMED CONSENT FORMS

The following steps should be performed if you are planning to archive paper informed consent forms at the archive in the Horst building:

1. During the research the informed consent forms are stored at a secure location (e.g. locker of the researcher).
2. When (parts of) the research is finished, the researcher fills in the information below ('Format archiving informed consent forms faculty ET). This information needs to be put on the outside of a sealed envelope that contains the informed consent forms.
3. This sealed envelope can be handed in at the secretary. The secretary contacts the archive (archive@utwente.nl) and stores the forms in a locker until they are picked up by the archive.
4. The archive picks up the forms and proceeds with the progress of archiving the informed consent forms in the Horst building.
5. If needed, the researcher(s) mentioned on the envelop can get access to the forms again after contacting the archive.

Format archiving informed consent forms faculty ET

Please fill in the information below and hand in the form together with the informed consent forms to the secretariat of the department / chair.

Faculty (abbreviation):	
Department (abbreviation):	
Chair (abbreviation):	
Name researcher:	
Title of the research project:	
Start date research project:	
End date research project:	
These documents should be destroyed at	DD-MM-YYYY
Reference number: *To be completed by the archive officer.*	