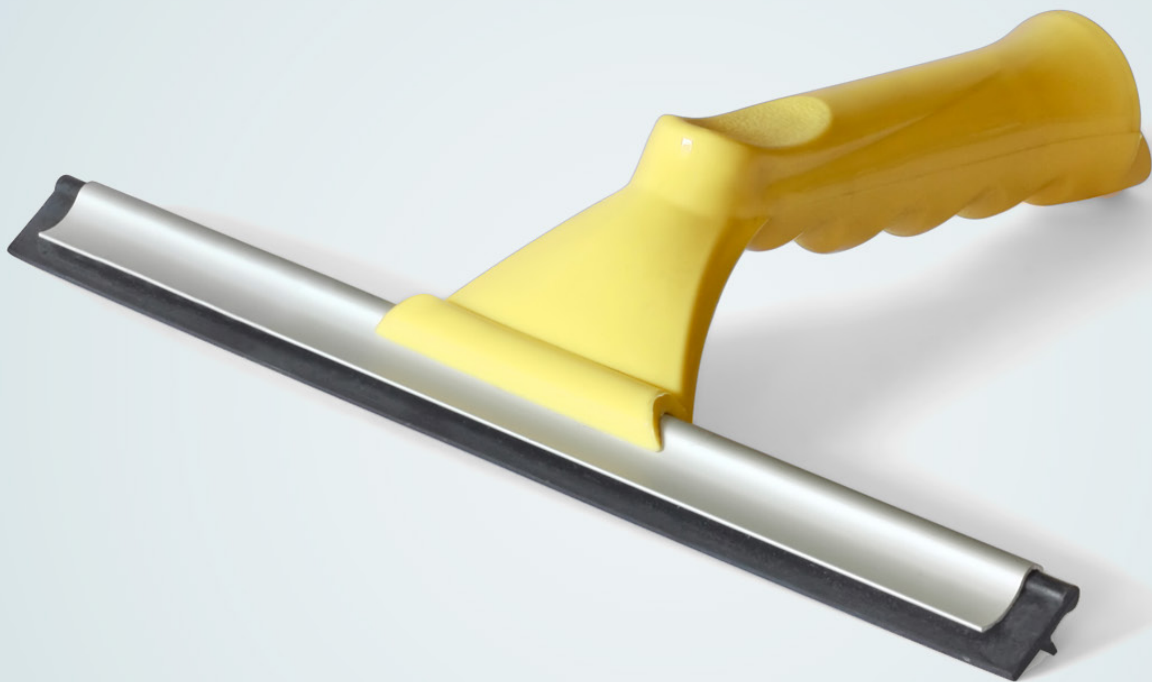


# Research Data and Software Management Policy

Version 3.0, 17-12-2024



# Information about this document

**Version:** 3.0

**Date of approval:** 17-12-2024

**Approved by:**  
VU Executive Board

**Evaluation:** This policy is being reviewed periodically and adjusted where necessary. The current version remains applicable until a new version has been released.

**Author:** Jolien Scholten

**In collaboration with** (in alphabetical order):  
Sander Bosch, Sam Heijnen, Tycho Hofstra,  
Marcel Ras, Dimitri Unger, Meron Vermaas

**Department responsible:** Network Research  
Data Support (NeRDS), University Library,  
department Research Support

---

If you have questions about this policy document, please contact [rdm@vu.nl](mailto:rdm@vu.nl).

The [Research Support Handbook](#) includes a page with references to VU-internal, national and international policies, principles and regulations on which this policy is based.

# Content

Introduction	1
Purpose	2
Policy principles	3
Responsibilities	4
Researchers	4
Department heads	5
Faculty boards	6
University	6
Terminology	8

# Introduction

Vrije Universiteit Amsterdam is strongly committed to the accessibility of research output, namely publications, data and software (see [Terminology](#)). They are important to the visibility, verifiability and reusability of research<sup>1</sup>.

The Research Data and Software Management Policy describes the university-wide principles for careful handling of research data and research software. At the level of the faculties, these principles are further developed into faculty policies and practical guidelines compliant with the central policy and describe processes that enable all departments and research institutes to comply with the central policy.

This policy applies to anyone who is involved in carrying out academic research for, or on behalf of, VU Amsterdam. This includes guest researchers.

<sup>1</sup> See also the [Vrije Universiteit's strategic plan](#).

# Purpose

The goal of the Research Data and Software Management Policy is to foster the careful management of [Research data](#) and [Research software](#), in order to:

- provide general guidance to researchers who want to make their data findable, accessible, interoperable and reusable ([FAIR Principles](#));
- foster transparency and enable verification, reuse and replication of research;
- handle research data and research software in a way that complies with legal requirements such as the General Data Protection Regulation (GDPR);
- assign responsibilities based on the Netherlands Code of Conduct for Research Integrity by Universiteiten van Nederland (*Universities of the Netherlands*, UNL)<sup>2</sup>, the FAIR principles for research data and relevant legislation.

This policy is in line with research assessment criteria as described in the Strategy Evaluation Protocol (SEP) 2021-2027, the San Francisco Declaration on Research Assessment (DORA), and the Coalition for Advancing Research Assessment (CoARA), as well as with the openness of research information as described in the Barcelona Declaration on Open Research Information.<sup>3</sup>

<sup>2</sup> See the [UNL website](#).

<sup>3</sup> References to these documents can be found in the [Research Support Handbook](#).

# Policy principles

1. Researchers must carry out their research according to the research integrity principles described in the Netherlands Code of Conduct for Research Integrity, drawn up by *Universiteiten van Nederland* (UNL).
2. Research activities must comply with all legislation and regulations where applicable, for example:<sup>4</sup>
  - General Data Protection Regulation (GDPR);
  - Implementation Act for the General Data Protection Regulation (UAVG);
  - Medical Research Involving Human Subjects Act (WMO);
  - Dutch Medical Treatment Contracts Act (WGBO);
  - Code of Conduct for Health Research;
  - Experiments on Animals Act.

<sup>4</sup> References to these regulations can be found in the [Research Support Handbook](#).

# Responsibilities

Ensuring good research data and software management practices is a shared responsibility in the university.<sup>5</sup> These responsibilities are explained below.

## Researchers

1. Researchers are responsible for complying with ethical requirements applicable to their research data and software (see also the [CARE principles for Indigenous Data Governance](#)), including review by ethics committees if necessary.<sup>6</sup>
2. Researchers are responsible for complying with legal requirements regarding their research data and software. Researchers who process personal data in their research must follow the privacy five-step plan and make sure that these activities are registered in the record of processing activities.<sup>7</sup>
3. Principal investigators must take appropriate measures to enable everyone in the research team to work according to the responsibilities described in this policy.
4. Researchers who reuse research data or software created by others must ensure that their reuse is permitted under the licences and (legal) conditions that apply. They must also make sure that the materials are cited or acknowledged in the correct manner.
5. Researchers are responsible for ensuring that their research data and software are reliably, traceably and securely stored (see [Data storage](#)) throughout the [Research life cycle](#).
6. Researchers are responsible for archiving (see [Data archiving](#)) all research data and software that leads to a published result (either in an article or other narrative form) in a [Trusted repository](#) for a period of at least ten years after this publication, unless legal requirements, discipline-specific guidelines or contractual arrangements dictate otherwise. The moment of publication is defined as the first online appearance of the publication. If there is no online publication date, the formal publication date of the publisher applies. Archived data and software<sup>8</sup> must contain everything that supports the published result, including appropriate documentation and metadata, so that the research process is transparent and verifiable.

<sup>5</sup> When working in a consortium, there is a shared responsibility of all consortium members to align all relevant policies. This should be addressed with the help of a consortium agreement.

<sup>6</sup> See the Research Support Handbook for an [overview of ethics committees](#).

<sup>7</sup> - [Privacy five-step plan](#): See the page [Working with personal data](#).

- [Instructions for registering the processing of personal data](#) in the record of processing activities can be found in the Research Support Handbook.

- The university (Stichting VU) is ultimately legally responsible for compliance with the applicable legislation, including the GDPR.

<sup>8</sup> A static copy of a software release version is important for being able to refer to this particular version in a publication. Having a static version also contributes to findability and citability in the long term. For software, it is useful to acknowledge the dynamic version as well, as this version can be maintained.

When datasets and software are archived in a repository provided by VU Amsterdam, the following requirements apply:

- the data and software must be provided with **Metadata** according to the VU Minimal metadata guide;<sup>9</sup>
  - the data and software must have a **Persistent identifier** (or Identifiers) to increase findability;
  - a licence must be applied to the data and software in order to indicate if it can be reused by others and if so, under which conditions.<sup>10</sup>
7. Researchers are responsible for publishing (see **Data publishing**) all research data and software that leads to a published result (either in an article or other narrative form) for scientific reuse, meaning that these materials can be discovered on the Web and referred to in a unique and persistent way. The level of accessibility to the data and/or software must be determined during the publication process. If data or software contain confidential information, information to which intellectual properties apply, and/or personal data, an assessment must take place to determine whether these data or software can be made available for reuse and if so, under which conditions.
8. Researchers are responsible for ensuring that a description of archived and published data and software is included in the 'Current Research Information System' (CRIS) of VU Amsterdam. In most cases, this is done automatically. Researchers should be able to provide information about data and software in an **Availability statement**.

## Department heads

9. Department heads are responsible for arranging agreements with researchers in their departments regarding the management of research data and software, particularly when a researcher's employment is ending.
10. When the PI is no longer available, department heads are responsible for deciding whether access can be granted to data and/or software that can only be made available upon request.

<sup>9</sup> **VU Minimal metadata guide**. In principle, richer metadata is better. However, the properties used in this guide should be applicable to a wide a range of tools, platforms etc. and outline the minimal information that should be provided about data.

<sup>10</sup> From the deposited data or software, it must be clear which conditions for reuse apply. Descriptions of standard licences that can be chosen in the repository, are in many cases automatically added to the archival package. Custom licences, which are particularly used for data or software that can only be made available upon request, must be added to the archival package manually.



## Faculty boards

11. Faculties must establish their own Research Data Management policies and/or operational guidelines, which are applicable to their departments and institutes.<sup>11</sup> For Research Software Management, faculty or departmental guidelines can be developed where necessary. Faculty policies and guidelines must be updated as required by new developments in or adjustments of the central Research Data and Software Management Policy.
12. Faculties are responsible for organising Research Data and Software Management support for researchers in their faculty, in collaboration with centrally-managed research support.
13. Faculties are responsible for replying to requests to verify data. They must develop a process for reviewing verification requests and providing the data.
14. The dean annually reports on compliance with their faculties' Research Data and Software Management policies and guidelines at the PO (*Portefeuillehoudersoverleg* or Portfolio Holder) meeting.

## University

15. The university is ultimately responsible for compliance with all applicable legislation (primarily the GDPR and UAVG) by each part of the university.<sup>12</sup>
16. The university is responsible for recognising and rewarding Research Data and Software Management, based on the Strategy Evaluation Protocol (SEP), San Francisco Declaration on Research Assessment (DORA), Coalition for Advancing Research Assessment (CoARA), and the Barcelona Declaration on Open Research Information.
17. The university is responsible for providing Research Data and Software Management services, including research infrastructure and professional support services.

<sup>11</sup> Depending on the size and structure of the faculties, these documents can take the form of policies in the sense of a framework that explains how more specific guidelines in the departments must be set up, or operational guidelines derived from the central policy directly. What is important, is that each faculty has operational guidelines in place for Research Data and Software Management, either at faculty, department or research institute level.

<sup>12</sup> First-line support to researchers regarding compliance with GDPR and UAVG is handled by the [Privacy Champions](#) in the faculties and services. Privacy experts at [Legal Affairs](#) function as second-line support. The [Data Protection Officer](#) monitors compliance with protecting personal data by VU Amsterdam and has an independent advisory role.

# Terminology

## Availability statement

Short description, usually included in a publication, of where data or software associated with a publication are available and under which conditions these materials can be accessed. Also known as (Data) Access Statement.

## CARE principles for Indigenous Data Governance

Principles for treating data about indigenous people in a responsible manner, addressing collective benefit (C), Authority to control (A), Responsibility (R) and Ethics (E).<sup>13</sup>

## Data storage concepts

**Data storage:** Safe and reliable storage of research data during the active research phase. Stored research data can be changed.

**Data archiving:** Creation of a secure and immutable copy of research data, associated metadata, accompanying documentation, and software code (where relevant) with the intention to ensure (conditional) access for a predetermined, minimum, period of time.

**Data publishing:** Making research data, associated metadata, accompanying documentation, and software code (where relevant) accessible in a repository in such a manner that **they can be discovered on the Web and referred to in a unique and persistent way**.<sup>14</sup>

## FAIR Principles

Principles for making research data Findable (F), Accessible (A), Interoperable (I) and Reusable (R).<sup>15</sup>

## Metadata

Data that describe characteristics of other data.<sup>16</sup> In the research context this concerns data that provide further information and context about research data. Metadata describe the data and the context in which they have been collected or created. See also [Research data](#).

<sup>13</sup> See the [Global Indigenous Data Alliance website](#) for more information and the [CODATA practice paper](#) [2020; DOI: <https://doi.org/10.5334/dsj-2020-042>] for a full publication on the CARE principles.

<sup>14</sup> Inspired by the definition in the CODATA Research Data Management Terminology, highlights by the author of this policy.

<sup>15</sup> See the [GO FAIR website](#) for a description of the FAIR Principles and the article by [Wilkinson et al.](#) [2016; doi:10.1038/sdata.2016.18] for an elaborate discussion.

<sup>16</sup> See the website of [Nationaal Archief](#).

## Persistent identifier

In short, and in the current context, a Persistent Identifier (PID) is essentially a URL that will never break.<sup>17</sup> There are multiple PID systems, each with its own particular properties. Examples of widely used PIDs in the research domain include.

**DOI:** A Digital Object Identifier can be used to refer to research data and research software. DOIs can be assigned to datasets and software upon their deposit in a repository.

**ORCID:** An Open Researcher and Contributor ID is used to create a researcher profile with a unique identification number. Researchers can request an ORCID themselves, with which they can identify their research output as their work.

**ROR:** The Research Organization Registry is a global register with persistent identifiers for research institutes. Researchers can use the ROR for VU Amsterdam when filling metadata forms for their research output to show that their work has been created within their employment at VU Amsterdam.

See the Persistent Identifier guide of [Netwerk Digitaal Erfgoed](#) for a more elaborate overview. Apart from widely used domain-agnostic PIDs, there is a wide range of domain-specific unique identifiers that can be used.

## Research data

Information that is captured for the purpose of underpinning academic research. Depending on the discipline it may consist of, for example, text, images, sound, spreadsheets, databases, statistical data, geographic data, etc. When we refer to research data in this policy, we refer to the entirety of the data itself, this includes any associated metadata and documentation.

## Research data management

“Research data management is an explicit process covering the creation and stewardship of research materials to enable their use for as long as they retain value.”<sup>18</sup>

## Research life cycle

The research life cycle outlines the various stages and activities of a research project, from preparation to disseminating the results.

<sup>17</sup> See [Netwerk Digitaal Erfgoed](#) for more information.

<sup>18</sup> See the Digital Curation Centre's [Glossary](#).

## Research software

“Research Software includes source code files, algorithms, scripts, computational workflows and executables that were created during the research process or for a research purpose. Software components (e.g., operating systems, libraries, dependencies, packages, scripts, etc.) that are used for research but were not created during or with a clear research intent should be considered software in research and not Research Software.”<sup>19</sup>

## Research software management

Research software management (RSM) is a structured and strategic approach to handling the creation, utilisation, and preservation of software in the research process.

## Trusted repository

“A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future.”<sup>20</sup>

<sup>19</sup> See the report [Defining research software: a controversial discussion](#).

<sup>20</sup> See the report [Trusted Digital Repositories: Attributes and Responsibilities](#), p. 5.

Research Data  
Management

[rdm.vu.nl](https://rdm.vu.nl)

