



**Universiteit  
Leiden**

# Faculty of Archaeology (FdA)

## Research Data Management Protocol

<b>Faculty</b>	Faculty of Archaeology (FdA)	<b>Version</b>	1.0
<b>Authors</b>	Adam K. Benfer Myrte T. Vos Jimmy Mans	<b>Date</b>	2026-01-30
<b>Contact</b>	rdm@arch.leidenuniv.nl		
<b>Status</b>	Approved	<b>URL/DOI</b>	10.5281/zenodo.18622276

# Table of Contents

<b>Section: Preamble to the Research Data Management Protocol</b> .....	1
<b>1. Introduction</b> .....	1
1.1 Research Data Management at Leiden University .....	1
1.2 Purpose of this Protocol .....	1
<b>2. To Whom this Protocol Applies</b> .....	1
<b>3. Definitions for Research Data Management</b> .....	2
3.1 What data are included in the scope of this protocol? .....	2
3.2 Research Data Management (RDM).....	2
3.3 Digital Research Data .....	2
3.4 Non-digital / Physical Research Data .....	3
3.5 Metadata and Documentation.....	3
3.6 Research Software .....	3
<b>Section: Planning and Preparing</b> .....	4
<b>4. Collaborations with Third Parties</b> .....	4
4.1 International Collaborations and Knowledge Security .....	4
4.2 Legal Agreements.....	4
4.3 Source Community and Indigenous Data Sovereignty .....	4
<b>5. (Re)Using Existing or Third-Party Data</b> .....	5
5.1 Intellectual Property Rights .....	5
5.2 Data Sharing Agreements .....	5
<b>6. Data Management Planning</b> .....	6
6.1 What is a data management plan (DMP)? .....	6
6.2 Who is expected to write, follow, and maintain a DMP?.....	6
6.3 DMP Templates.....	6
6.4 Writing the DMP .....	6
6.5 Reviewing and approving the DMP .....	7
6.6 When to update/revise the DMP? .....	7
6.7 Procedures for Registration, Storage, and Archiving of the DMP .....	7
6.8 Relation of DMP to Other Relevant Procedures and Documents.....	7
<b>Section: Protecting and Processing</b> .....	9
<b>7. Secure Management of Data</b> .....	9
7.1 Data Storage .....	9
7.1.1 Data Storage Options at Leiden University .....	9
7.1.2 Post-Contract Data Destruction at Leiden University.....	9
7.2 Data Transport and Transfer.....	9

7.3	Data Documentation .....	9
7.4	Version Management .....	10
7.5	Data Formats .....	10
<b>Section: Preserving and Publishing .....</b>		<b>10</b>
<b>8.</b>	<b>Research Data Underlying a Publication.....</b>	<b>10</b>
8.1	Archiving Data Underlying Publications.....	10
8.2	Selection Criteria for Data Publication and Archiving.....	10
8.3	Preferred / Certified Repositories .....	11
8.4	Choosing a Usage License .....	11
8.5	Data Access Protocol for Restricted Datasets .....	11
8.6	Registering Published Research Data with LUCRIS.....	12
<b>9.</b>	<b>Research Data Not Underlying a Publication.....</b>	<b>12</b>
9.1	Archiving Data Not Underlying Publications .....	12
9.2	Archiving Data Underlying BA, MA, and RMA Theses.....	12
<b>10.</b>	<b>Archiving Legacy Data .....</b>	<b>13</b>
10.1	Preparing for End-of-Contract or Retirement .....	13
10.2	Preserving Non-Digital Data.....	13
10.3	Archiving a Personal Non-Digital Data Collection.....	13
<b>11.</b>	<b>Retention Periods.....</b>	<b>13</b>
<b>Section: Roles and Responsibilities .....</b>		<b>14</b>
<b>12.</b>	<b>Responsibilities.....</b>	<b>14</b>
12.01	Executive Board .....	14
12.02	Faculty Board .....	14
12.03	Executive Director of Research .....	14
12.04	Policy Officer of Research.....	15
12.05	Policy Officer of Research Data (Faculty Data Steward) .....	15
12.06	Department Head .....	16
12.07	Principal Investigator.....	16
12.08	Supervisors .....	17
12.09	Project, Facility, or Laboratory Managers.....	17
12.10	The Researcher .....	17
<b>13.</b>	<b>Where to Find Support.....</b>	<b>18</b>
13.1	Faculty Support Staff.....	18
13.2	Central Support.....	18
13.3	Training and Information.....	18
<b>14.</b>	<b>Reporting Incidents .....</b>	<b>18</b>

14.1	Data Loss or Corruption.....	18
14.2	Data Leaks.....	18
<b>15.</b>	<b>Procedures for this Data Protocol .....</b>	<b>18</b>
<b>Appendix 1: Relevant Legislation and Agreements.....</b>		<b>20</b>
1.1	National Legislations and Guidelines.....	20
1.2	University Guidelines.....	20
1.3	Faculty-Specific Guidelines and Protocols .....	20
1.4	International .....	20
1.5	Other Guidelines .....	20

## Section: Preamble to the Research Data Management Protocol

### 1. Introduction

Research data are the driving force behind academic research. Therefore, good data management throughout the research lifecycle improves the transparency, integrity, reproducibility, and reach of scholarly research. It benefits the researcher, by supporting their workflow and mitigating the risk of accidental data loss; their research community, by maximizing the utility and reusability of data, and protecting participants and interlocutors against data leaks and safeguarding their privacy and safety; and finally, society at large, by ensuring long-term access to research data and making it available as a public good.

#### 1.1 Research Data Management at Leiden University

Individual researchers and institutions—including funding agencies such as NWO and Horizon Europe—are increasingly committed to making publicly funded research available through Open Access publishing, and archiving research data under the principle “as open as possible, as closed as necessary”. The Netherlands Code of Conduct for Research Integrity (2018) lays out researchers’ responsibilities with regards to data management, and institutions’ duties of care in providing the necessary information, infrastructure, storage capacity, and support.

The Executive Board of Leiden University has formulated regulations applying to all digital and physical (non-digital) data used and generated during academic research (the Leiden University Research Data Management Regulations [RDM2021]).<sup>1</sup> These regulations are intended to provide a framework for a university-wide research data management policy for which further elaboration will be initiated at the faculty and institute levels.

As research is among its core activities, the Faculty of Archaeology (henceforth “the Faculty”) endorses the University mission for effective research data management. This document presents a specific research data management (henceforth “RDM”) protocol for the Faculty that translates and elaborates upon the clauses of the RDM2021 to present concrete implementation guidelines specifically pertaining to the types of research and practice in the Faculty.

#### 1.2 Purpose of this Protocol

This data protocol aims to clarify the responsibilities of individual researchers and other stakeholders throughout the Faculty, and to encourage best practices in research data management. It is intended for researchers who are starting a research project within the Faculty for which a data management plan may be drawn up and/or will submit a proposal to external funders or to the Ethics Committee in which data management may play a role. This document is binding for projects starting after the date on which a final version of this elaboration has been adopted by the Faculty Board. In cases not covered by this elaboration, the Executive Director of Research in consultation with the Faculty Board is authorized to make decisions.

While this protocol describes discipline-specific data management requirements linked to established research practices within the Faculty, the protocol was developed using a common, University-wide template to ensure a coherent approach to data management across Leiden University. Intended to be a ‘living document’, this protocol will be regularly updated as best practices around research data management evolve and Leiden University continues to elaborate and improve its support infrastructures.

The data protocol is not meant as a guide for researchers, but rather as a formalization of the obligations of research and support staff within the Faculty. Additional guidance and non-normative advice are provided within the [Faculty Data Management Handbook](#).

### 2. To Whom this Protocol Applies

In line with §3 of RDM2021, the regulations contained within this protocol apply to all employees and persons affiliated with the Faculty, including contract PhD candidates, external PhD candidates, research assistants, retired colleagues, visiting researchers, and other guests or partners who carry out research under the auspices or sponsorship of the Faculty. Research conducted by bachelor’s and (research) master’s students fall under the formal responsibility of their supervisors: the data protocol only applies to them if and when their research

---

<sup>1</sup> Leiden University [Data Management Regulation](#)– version 1.0, 7-12-2021.

results in an academic publication or is reused in another research project (in which case they should also be properly credited).

### 3. Definitions for Research Data Management

#### 3.1 What data are included in the scope of this protocol?

This protocol scopes over all materials and information, digital and physical, that are collected or provide the basis for analysis in academic research, and that is necessary to substantiate and validate the outcomes of that research. This includes data in all stages of the research lifecycle—raw (unprocessed), derived (processed), and analysed—and the methods by which they are transformed from one stage to the next. It also includes research software that is developed during the research—to support data collection, processing, and analysis, or as research output in its own right—and supporting documentation such as stimuli, codebooks, readme files, field notes, audit trails, statement of approval from the ethics committee, proof of informed consent, etc.

This scope is deliberately defined as broadly as possible, to be inclusive of the full range of epistemologies, methodologies, and research outputs found in archaeology. It is primarily informed by what is needed to meet the twin responsibilities of the researcher to 1) corroborate claims with evidence, and 2) do so honestly, scrupulously, and transparently. Secondarily, it is aligned—where possible and reasonable—with the aspirations of the Open Science movement, striving to manage data such that they are accessible and interpretable to the widest possible audience. What follows in this section are a series of definitions related to Research Data Management within the Faculty.

#### 3.2 Research Data Management (RDM)

Research Data Management is the careful organization and management of research (meta)data, in both digital and non-digital format, and research software throughout the research cycle.

#### 3.3 Digital Research Data

- 3.3.1 **Research data** are “a relational category applied to research [inputs and] outputs that are taken, at specific moments of inquiry, to provide evidence for knowledge claims of interest to the researchers involved.”<sup>2</sup> This is understood as all information that is produced, generated, collected, acquired (licensed as open or restricted), gathered, processed, analysed, and (re-)used during academic research, commonly accepted in the scientific community as necessary to validate research findings. From here on, ‘data’ refers to ‘research data’ unless otherwise specified.
- 3.3.2 All data produced, generated, collected, acquired, gathered, and purchased by Faculty employees are owned by Leiden University unless otherwise specified (see Contract research data (§3.3.6) and Indigenous Data Sovereignty (§4.3))<sup>3</sup>.
- 3.3.3 **Raw research data (unprocessed data)** are data that arise (e.g., are produced, generated, collected, acquired, gathered) from observation, experimentation, or simulation for the purpose of scientific analysis (i.e., data that are not derived from other research data).
- 3.3.4 **Derived research data (processed data)** are data that arise from processing or analysing raw research data.
- 3.3.5 **External/third-party research data** are research data owned by an external or third-party (see §5.1 on Intellectual Property Rights).
- 3.3.6 **Contract research data** are external/third-party research data collected by Leiden University employees under contract by an external or third-party (see §5.1 on Intellectual Property Rights).
- 3.3.7 **Confidential research data** are research data intended for (or restricted to) the use of a particular person or group and/or contains information whose unauthorized disclosure could be harmful to the University and/or its stakeholders.

---

<sup>2</sup> Leonelli, Sabina. “What Counts as Scientific Data? A Relational Framework.” *Philosophy of Science* 82 (2015): 810–821. <https://doi.org/10.1086/684083>; Leiden University [Employer Copyright Regulations](#) – version 1.0, 4-2-2025, page 1

<sup>3</sup> Leiden University [Employer Copyright Regulations](#) – version 1.0, 4-2-2025, page 3

- 3.3.8 **Personal data in research** refers to any research data that can lead to the identification, directly or indirectly, of a person, including but not limited to name, signature, address or location, telephone number, an identification number, an online identifier or any factors specific to the physical, physiological, genetic, biometric, mental, economic, cultural or social identity of that person.
- 3.3.9 **Special categories of personal data in research** are personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or uniquely identify, directly or indirectly a person, including their health, sex life, or sexual orientation. Unless a specific exception applies, the GDPR prohibits the processing of these data.<sup>4</sup>
- 3.3.10 Within the research data lifecycle, three types of data are distinguished from the storage perspective.
- 3.3.10.1 **Working data** are all research data (raw and derived) that are frequently accessed and actively used during ongoing research.
  - 3.3.10.2 **Internally archived data** are all research data (raw and derived) that the researcher deems valuable to preserve yet are not frequently accessed nor actively used during ongoing research. Internally archived data are understood as archived on Leiden University approved regular storage or dedicated archive storage.
  - 3.3.10.3 **Published data (publicly available data)** are all internally or externally archived data that the researcher shares publicly either directly or as a copy.

### 3.4 Non-digital / Physical Research Data

Non-digital Research Data are all physical or analogue research inputs or outputs, such as field notes, field forms, laboratory notes, laboratory sheets, drawings, etc. As defined here, Non-digital Research Data do not include the samples, artifacts, ecofacts, or other physical objects of analysis that may be described or characterized by data.

### 3.5 Metadata and Documentation

- 3.5.1 **Research metadata** are standardized structured data that are necessary to describe research data and research software to be understood by humans and machines. Metadata may be produced manually by a researcher or automatically by research instruments.
- 3.5.2 **Research documentation** is a descriptive introduction and/or overview of research that is necessary to understand research (meta)data and research software by humans including descriptions of processes, equipment, and set-ups used.

### 3.6 Research Software

- 3.6.1 **Research software** is software developed to produce, generate, collect, acquire, gather, process, analyse, and (re-)use research data (i.e., software for the purpose of simulations, statistical analyses, or visualizations).
- 3.6.2 All research software developed by Faculty employees and/or students participating in research initiated by the University is owned by Leiden University.
- 3.6.3 **External / Third-party research software** is research software owned by an external or third-party.
- 3.6.4 **Internally archived research software** is all research software that the researcher deems valuable to preserve yet is not frequently accessed nor actively used during ongoing research.
- 3.6.5 **Published research software (publicly available research software)** is all research software that the researcher shares publicly.

---

<sup>4</sup> Ministerie van Justitie en Veiligheid, *Handleiding Algemene verordening Gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming* (The Hague: Ministerie van Justitie en Veiligheid 2023), art. 3.2.1, 24.

## Section: Planning and Preparing

### 4. Collaborations with Third Parties

#### 4.1 International Collaborations and Knowledge Security

Collaboration, both national and international, brings interesting research opportunities, but might also bring risks: misuse or theft of knowledge, ethical issues associated with the application of research results, uncertainties about archiving roles/responsibilities, or unwanted interference that affects academic freedom. The initiator (usually the Researcher or Principal Investigator) must discuss any proposed international collaboration with their Department Head and Faculty's Policy Office of Research using the office Knowledge Security consultation questionnaire.<sup>5</sup> During this consultation, if the Department Head determines that the risks of the proposed collaborative initiative are substantial and/or complex, the collaboration should be cancelled or adjusted to mitigate these risks, or the University's Knowledge Security Advice Desk may be consulted. However, if the initiator disagrees with the assessment of the Department Head, the University's Knowledge Security Advice Desk must be contacted ([email](#)). Thereafter, the University's Knowledge Security Committee will assess the potential risks and opportunities of the proposed collaborative initiative and issue a binding decision to the initiator with four weeks.<sup>6</sup> For more details, see the University policy on [Knowledge Security](#).

#### 4.2 Legal Agreements

When collaborating with external or third parties (be it other universities, public or government institutions, private companies, etc.), clear agreements need to be made on how research data will be collected, processed, accessed, used, and stored, as well as on intellectual property rights, such as co-authorship<sup>7</sup>, copyright<sup>8</sup>, and terms of use.

In cases of collaborative research with such third parties, a Collaborative Agreement should clearly and appropriately delegate all RDM responsibilities. Unless otherwise specified in a Collaborative Agreement, Data Sharing Agreement (DSA), or other legal agreement, the RDM terms and conditions outlined in this protocol should be followed by all research staff of the Faculty who are collaborating with third parties.

The University's Knowledge Exchange Office ([LURIS](#)) can help researchers generate some legal agreements such as a Confidentiality Disclosure Agreement (CDA), a Material Transfer Agreement (MTA) for non-human material, or a Consultancy Agreement. For some legal agreements, such as a Data Processing Agreement (DPA), a Data Transfer Agreement (DTA), a Data Sharing Agreement (DSA), or a Joint Controller Agreement (JCA), the Privacy Office has [templates](#) available that researchers may use to keep in compliance with the GDPR. For other legal agreements, LURIS can offer advise and help the researcher draw up a contract if deemed necessary.

When the collaboration involves personal data as defined by the GDPR, it is very likely a DSA or JCA is required: contact a [Privacy Officer](#) as early as possible. See §6.8.2 for more information.

When collecting personal data *through* a third party (i.e., where the researcher is the data owner, and the third party is the data processor), the researcher may need to draw up a DPA to comply with the GDPR. A Privacy Officer can determine whether this applies to the research project; if so, they can help the researcher draw up a DPA. Online data collection tools and platforms for which the University has a license (e.g., Qualtrics) may not require the research to draw up a DPA.

Note that the researcher rarely has the mandate to sign legal agreements themselves. Contact the [Policy Officer of Research](#). Also see §5.2 on Data Sharing Agreements with respect to the re-use of third-party data.

#### 4.3 Source Community and Indigenous Data Sovereignty

Researchers at the University are obliged to conduct their research involving people in accordance with the principles of the GDPR, and to take the rights of living "data subjects" into account.<sup>9</sup> This already gives research

---

<sup>5</sup> Leiden University [Policy Framework for Knowledge Security](#) – version 1.0, 19-12-2024, page 22–27.

<sup>6</sup> Leiden University [Policy Framework for Knowledge Security](#) – version 1.0, 19-12-2024, page 12–13.

<sup>7</sup> Faculty of Archaeology (Leiden University) [Co-authorship Considerations and Guidelines](#) – version 1.0, 18-5-2021.

<sup>8</sup> Leiden University [Employer Copyright Regulations](#) – version 1.0, 4-2-2025.

<sup>9</sup> [General Data Protection Regulation](#) (Regulation (EU) 2016/679 of the European Parliament), art. 4(1).

participants in source communities a relatively high degree of control over their personal data. However, some forms of research consider participants the (co-)owners of data gathered about them, or as co-creators of the research methodology and published output; or involve communities that assert authority to control data about them (see e.g., the CARE Principles for Indigenous Data Governance<sup>10</sup> and IEEE 2890-2025<sup>11</sup>). Such participant groups and source communities may have a history of being exploited, mischaracterized, and marginalized by scientific research. In such cases, the researcher usually holds the research data ‘in trust’, and needs to not only proactively negotiate agreements around data access, licensing, publication, preservation, and authorship, but also centre collaborators’ needs and perspectives with regards to their data (e.g., in the choice of metadata terms or codes used during data analysis). In such cases, the Faculty recommends that researchers utilize Local Context Labels and Notices throughout their research outputs. For more information on research ethics see §6.8.1 on Ethics Review and §6.8.2 on Research Data Privacy.

For all data that have been collected from an Indigenous community, whether that be knowledge, immaterial, visual, and/or material culture, the University is not the owner but the holder of the data. The rights of the relevant Indigenous community take precedence and their wishes regarding how that data are to be handled throughout the research lifecycle must be respected.<sup>12</sup>

## 5. (Re)Using Existing or Third-Party Data

### 5.1 Intellectual Property Rights

Third-party research data (see §3.3.5) are any data that have been created by other researchers or by external agents, such as census data created by Statistics Netherlands or data collected by contract archaeologists. These data may be sourced directly from the creator, or from secondary sources such as articles, books, corpus databases, and repositories. Third-party data may be protected by intellectual property rights such as licenses, copyright, patents, and trademarks. If researchers reuse third-party data, they should be aware of any restrictions.

Two exceptions to the Dutch copyright law<sup>13</sup> are particularly relevant to researchers using digital research methods:

- You may make a private copy of a copyrighted work for research purposes,<sup>14</sup> and
- You may reuse copyrighted material that you have legal access to, for the purpose of text and data mining. You must store reproductions with appropriate security measures, and you may preserve them for academic research purposes (e.g., verification and replication of results).<sup>15</sup>

Instead of an owner, research data usually have a ‘rights holder’ who determines its license and who may need to be asked for permission to reuse and publish it. Leiden University is generally the ‘rights holder’ of research data created under its employ (though this may depend on the specific contractual agreement with the researcher).<sup>16</sup> In practice, researchers often set the license on their data and make decisions on how openly it is published (see §8.4).

When extracting or re-using data from copyrighted publications (books, articles, artworks, etc.), the Copyright Information Office at the University library can help you navigate the terms of use. They can also give advice on asserting intellectual property rights on your own work.

### 5.2 Data Sharing Agreements

When handling third-party data, a license or written permission needs to be obtained from the relevant third party. This can be part of relevant agreements, such as a Data Sharing Agreement (see §4.2). To determine the

---

<sup>10</sup> Global Indigenous Data Alliance, *CARE [Collective benefit, Authority to control, Responsibility, and Ethics] Principles for Indigenous Data Governance*.

<sup>11</sup> IEEE *Recommended Practice for Provenance of Indigenous Peoples' Data* (IEEE [Institute of Electrical and Electronics Engineers] 2890-2025).

<sup>12</sup> Leiden University *Employer Copyright Regulations* – version 1.0, 4-2-2025, page 5.

<sup>13</sup> *Auteurswet* [Copyright Law] (Ministerie van Justitie 2025).

<sup>14</sup> *Auteurswet* [Copyright Law] (Ministerie van Justitie 2025), art. 16b-c.

<sup>15</sup> *Auteurswet* [Copyright Law] (Ministerie van Justitie 2025), art. 15n-o.

<sup>16</sup> Leiden University *Employer Copyright Regulations* – version 1.0, 4-2-2025, page 3.

agreements to be drafted legal advice needs to be requested through the Research Support Office. Although LURIS provides the legal advice, the Research Support Office is to be involved to ensure the documents are compliant.

Note that when the third-party data involve personal data, the providing party must first confirm that they can lawfully share the personal data with the researcher.

## 6. Data Management Planning

### 6.1 What is a data management plan (DMP)?

A data management plan (DMP) is a formal statement describing how research data and research software will be managed and documented throughout a research project and the terms regarding the subsequent deposit of the data/software in a repository for long-term management and preservation.

A good DMP offers many benefits: it can structure conversations and aid decision-making about research workflows, especially in project teams and consortia, which saves time and mitigates the risk of costly misunderstandings and mistakes. It helps the researcher and their community (both in- and outside academia) to get the most out of valuable research data. Finally, it is a useful instrument in supporting research integrity.

### 6.2 Who is expected to write, follow, and maintain a DMP?

Per RDM2021, **all** researchers at Leiden University are expected to create a DMP at the beginning of the research process. In practice, the Faculty applies this policy as follows:

- PhD candidates and grant-funded researchers are **required** to write a DMP for their project.
- Research projects which rely on well-documented source material and do not generate new research data, are **exempt**.
- Researchers who are conducting research which is not externally funded, not intended for publication, and/or not linked to a specific project are **encouraged** to plan and document their data management strategy in whatever way best supports their work.

### 6.3 DMP Templates

Researchers in the Faculty are encouraged to use the [Leiden University DMP template](#). Most funders, including NWO, ERC, and Marie Curie, accept this template. If this is not the case, the researcher should use a template provided by the funder of their research. In the case of larger collaborations or consortia, the researcher may have to work with a template from a project partner.

### 6.4 Writing the DMP

The researcher is responsible for writing the DMP, a first draft of which should be written before the research project starts, but no later than two months after the start of the research project. The collaborators and, if relevant supervisors and other colleagues participating in the project, must be involved in the discussion leading to the chosen Research Data Management strategy that underlies the DMP writing process. For research funded by grants, the DMP should be written in accordance with the funder's requirements. Researchers are requested to contact and discuss their DMP with the Faculty [Data Steward](#) to receive discipline-specific advice and support during the writing process.

A research project, no matter how large, should have *only* one 'active' DMP. In the case of research teams and consortia, it should be clearly agreed which research partner will be in charge of the overarching project DMP. Depending on the project, it may be practical to devolve certain aspects of data management planning down to the level of partner organizations or individual researchers, but this division of labour should be clearly outlined in the top-level DMP. Among other responsibilities, the DMP should indicate who is responsible for depositing the research data at the end of the project, archiving any other data that are not deposited, and deleting any (personal) research data, if necessary. PhD candidates working on their dissertation project within a larger research project are advised to submit the current version of that project's DMP alongside their Training and Supervision Plan (TSP), and to summarize the parts of it that are relevant to their work package within the TSP. Postdoctoral researchers are encouraged to follow the same procedure.

For research based on the same methodology, the Faculty suggests that researchers agree on a set of standardized research data management protocols that are outlined within an umbrella DMP, which all researchers using that methodology may follow. These standardized protocols should harmonized research data management practice while allowing for appropriate flexibilities. The exact nature of the methodology must be clearly defined in the umbrella DMP. Such umbrella DMPs should then be updated regularly as research methods and best practices change or evolve.

#### 6.5 Reviewing and approving the DMP

For grant-funded researchers, review and approval of their DMP by a local Data Steward is commonly required by the funder. Note that the approval of the DMP will not set its text in stone as it is a living document.

DMPs for PhD research should be approved by the Data Steward as a mandatory part of the Archaeological Research Data Management course and subsequently approved and signed by the project's primary supervisor.

#### 6.6 When to update/revise the DMP?

The DMP should be a living document that adapts and refines as the research project progresses, develops, and evolves. The researcher is advised to review the DMP every year and expected to update the DMP if applicable. Revisions of the DMP should occur in such cases as the following:

- A significant deviation in the research methodology used.
- A significant method or process change such as a modification of the data storage solution.
- A structural change in the project outline such as a new PhD project starting or the need to add a further different study to the project.

Whenever a significant change is made in the research project, the DMP needs to be updated and the Data Steward notified.

#### 6.7 Procedures for Registration, Storage, and Archiving of the DMP

The researcher is responsible for submitting each version of the DMP and all related documents mentioned in this protocol to the Faculty [Data Steward](#). Researchers who are required to write a DMP (see §6.2) are also *required* to submit, store, and ensure the availability of their DMP during the 20-year retention period stipulated by RDM2021 (§15).

- PhD candidates are required to submit their signed DMP, as well as later updated versions, to the Data Steward who will in turn keep the Graduate School informed. The most recent copy of the DMP is kept within the candidate's file in the Faculty RDM SharePoint. At the end of the PhD project, the final version of the DMP is archived internally, while the dissertation and the associated research data are archived in their respective publicly accessible repositories.
- Grant-funded researchers may be required to submit their DMP to their funder (usually either before the project starts or within 4 months of when the grant is awarded). Updated versions of the DMP are clearly named as such and kept on file with the project administration. The final version of the DMP is archived (until further notice) with the Faculty Data Steward, and (if required) submitted to the funder as part of the final report.

University-wide tooling for the registration and storage of DMPs is currently under development as of January 2026. So long as this tooling is not available, the Faculty *encourages* researchers to write a DMP for their research workflow and store it alongside other vital project administration documents. Researchers can send their DMP to the Data Steward who will then archive it on the Faculty's RDM SharePoint.

#### 6.8 Relation of DMP to Other Relevant Procedures and Documents

Data management planning, particularly for research that will involve human subjects and/or processing personal data, is closely entwined with data privacy and security considerations - which in turn form an important part of the Ethics Committee's review criteria. Researchers planning to apply to the Ethics Committee for review and approval of their project, must first write a DMP. Projects involving personal data will need vetting, and potentially also tailored advice, from a [Privacy Officer](#) before the Ethics Committee can review them; this process goes smoother and faster when the Privacy Officer has access to a DMP.

### 6.8.1 Ethics Review

The Faculties of Humanities and Archaeology share an [Ethics Committee](#). Researchers who are planning to work with human subjects or human remains; collect, process, or analyse living people's personal data; and/or analyse cultural heritage artefacts and materials, are required to submit their planned research to the Committee for review. Ethical review is optional for (Research) Master students, but recommended if the intent is for their research to be published, and/or if they conduct their research using facilities provided by the Faculty.

Researchers present their research for review through the application form (downloadable through the website), plus any relevant supporting documentation, such as their DMP, acquired archaeological fieldwork permissions, an information and consent form, proposed survey questions, etc.

See the Committee's website and [checklist](#) to determine whether your research needs to be submitted for review. Questions and applications can be sent in to the [Ethics Committee](#).

### 6.8.2 Research Data Privacy

A [Privacy Quicksan](#) is a list of questions used to determine the level of risk of privacy infringement and data leaks in a research project. If during the course of proposed research, a researcher intends to process (that is to collect, store, change, share, view, or delete) personal data (meaning data that says something about a person that may make it possible to directly or indirectly identify that person), the researcher should complete a [Privacy Quicksan](#) and submit it to the [Privacy Service Point](#). A Privacy Officer will then review the information provided in the form and suggest mitigation measures. Depending on the proposed research, the Ethics Committee may also need to be involved in those process.

If the risks are deemed high, it may be necessary to carry out a **Data Protection Impact Assessment (DPIA)**. High risk, in this context, means something else than just confidential or sensitive personal data, or personal data collected under high-risk conditions (e.g., a warzone, a domestic abuse shelter, etc.). A DPIA is called for when you plan to, for example, process large volumes of 'special category' personal data (e.g., ethnicity, religious beliefs, sexual orientation, etc.), evaluate people and/or make decisions about them based on automated profiling, or do large-scale monitoring of people in a public space. A DPIA is also recommended if researchers are working with new methodologies or technologies whose impact on the privacy of "data subjects" is not yet clear.

Note that guest researchers and external PhD candidates are not contractual employees of Leiden University; therefore, the University is not formally, legally responsible for these researchers' compliance with the GDPR. Instead, the researcher or the external institution in which they are based/work is the entity that must guarantee compliance with the GDPR. However, the Faculty of Archaeology acknowledges its duty of care to all affiliated researchers, and encourages external PhD candidates and guest researchers to reach out for support and advice tailored to their situation.

For a comprehensive guide on data privacy for research, see Utrecht University's [online handbook](#).

### 6.8.3 Code of Conduct for Fieldwork

All staff, researchers, and students of the Faculty who are engaged in archaeological fieldwork are obliged to comply with the Faculty's Code of Conduct for Fieldwork.<sup>17</sup>

When going on fieldwork or other research abroad, the researcher should make themselves familiar with the legal and regulatory situation in the countries in which they will conduct research and/or through which they will travel. In addition to checking how such international agreements as [The Nagoya Protocol on Access and Benefit Sharing](#) and [CITES \(the Convention on International Trade in Endangered Species of Wild Fauna and Flora\)](#) might influence their fieldwork, the researcher should also check the [UNESCO Database of National Cultural Heritage Laws](#) to verify that they are complying with all relevant national cultural heritage laws and pay special attention to the growing number of laws pertaining to data governance that may relate to the research data that they will collect and/or obtain.

The researcher should also be aware they might be exporting personal data to a different jurisdiction. The researcher should ask for consent for this, and not take the data if the consent is not given. The researcher should also be aware that, while working abroad, their actions are still covered by the GDPR.

---

<sup>17</sup> [Code of Conduct for Fieldwork in the Faculty of Archaeology](#) – version 2.0, 1-9-2023.

For a comprehensive overview of things to consider when collecting data ‘in the field’, please consult Leiden University’s [checklist for Data management while working abroad](#).

## Section: Protecting and Processing

### 7. Secure Management of Data

#### 7.1 Data Storage

The choice of storage location should depend, first and foremost, on the sensitivity and protection needs of your data. A *confidentiality, integrity and availability* classification (CIA; in Dutch: BIV-classificatie) of data storage options at Leiden University is under development at the time of publishing this protocol.

Additional safety measures need to be taken for the storage/handling of confidential or sensitive (personal) data, including data that constitute a security risk for the University or other parties. As of the current version of this protocol, Leiden University does not offer appropriately secure storage for high-risk sensitive data. Contact [support staff](#) to discuss alternative solutions.

##### 7.1.1 Data Storage Options at Leiden University

The University’s internal storage provision (i.e., the J:drive) is currently being slowly phased out. It is recommended to use the institutional Microsoft 365 applications (OneDrive, Teams, Sharepoint) and SURF applications (SURFdrive, Research Drive, and Yoda).

By default, guest researchers and external PhD candidates have limited access to the University’s ICT resources. Nonetheless, the security needs of their data may require a managed device, encrypted storage, specialized software, or other measures. Contact the Faculty [Information Manager](#) to discuss available options.

##### 7.1.2 Post-Contract Data Destruction at Leiden University

Note that the University’s ‘grace period’ for departing researchers’ UCLN accounts is 60 days (two months) after the end of contract. After this period, the account and its associated stored data are deleted. A departing researcher and their supervisor have a joint responsibility to negotiate and transfer stewardship of any (copies of) research data that were collected or generated during the researcher’s employment term. These terms should be clearly detailed in the project DMP. See §10.1 for more information.

#### 7.2 Data Transport and Transfer

In compliance with University cybersecurity policy<sup>18</sup> and general best practices, researchers should transfer data directly, or as quickly as possible, to their recommended/approved data storage solutions. When transporting or transferring sensitive data, the device or transfer protocol must use encryption.

University-managed hardware and software should be used wherever possible. When sharing files with other researchers, use SURFdrive, SURF Research Drive, or SURFFileSender. While SharePoint or OneDrive may be used for sharing research data within the University, it is not recommended for use when sending or receiving research data with external collaborators. Do not use non-managed options such as Google Drive, Dropbox, or WeTransfer. Contact the Faculty [Information Management](#) office if you have questions or need assistance.

#### 7.3 Data Documentation

Stored datasets need to be well documented. This includes a brief description of the dataset (metadata properties), an overview describing individual files, and (where applicable) codebooks describing data elements used and descriptions of code syntax. Clear and transparent documentation helps save time both during and at the end of a research project, when data are prepared for publishing and archiving.

Software should be presented with relevant metadata that encompass at minimum: the creators of the software, the name of the software, the date the software was published, the identification of whom is responsible for

---

<sup>18</sup> Leiden University [Strategic Policy on Information Security 2023–2027](#).

software upkeep, the Creative Commons license, the identifier (if no persistent identifier is linked to the software, the URL – for example for software on GitHub), and the version.

#### 7.4 Version Management

Proper version management should be practiced such that the original (raw, unmodified) version of the data can always be identified; versions of the data that constitute the basis for specific publications can be identified; and errors when working with the data can be mitigated so that a minimum (e.g., one day's worth) of work is lost.

Exceptions from this general guidance (for instance because of the size of a dataset or security concerns) should be motivated in a DMP.

#### 7.5 Data Formats

Data should be archived using file formats that offer the best long-term guarantees for usability, accessibility, and sustainability. As a general guideline, such preferred formats:

- Have open specifications;
- Are frequently used;
- Are independent of specific software, developers, or vendors.

For example, use .odt, PDF/A, or .txt file formats for text documents rather than .doc(x) or .rtf; .csv for tabular data instead of .xls(x); etc. While file formats that do not meet these criteria may be necessary during the course of your research, you should convert them to sustainable formats at the end of the project.

In practice, it is not always possible to use formats which satisfy all of these criteria. In certain cases it may be desirable to archive data in 'non-preferred formats' instead of (or ideally in addition to) preferred formats: i.e., formats that are widely used in your field, and which will be moderately to reasonably usable, accessible, and robust in the foreseeable future.

The Dutch national institute for Data Archiving and Networked Services (DANS) maintains a list of preferred file formats [here](#).

### Section: Preserving and Publishing

## 8. Research Data Underlying a Publication

### 8.1 Archiving Data Underlying Publications

The RDM2021 mandates that all digital (research) data underlying a scientific publication are to be archived/deposited in a trusted and (preferably) certified research data repository. A publication with an associated dataset should include a persistent identifier to the archived dataset, and vice versa.

The first and foremost purpose of archiving data is to support the principles of research integrity, by facilitating the verification of researchers' claims. By publishing data, researchers also contribute to a more open, sustainable, and equitable research landscape, by making their data easier to access (including by non-academic audiences), cite, and reuse.

There may be legal, ethical, commercial, political, environmental, or cultural reasons for not sharing data openly/publicly, including but not limited to personal data protection, intellectual property rights, knowledge security risks, and (indigenous) communities' authority to control data from or about them. When it is not possible to archive data with open/public access, they should be archived with restricted or closed access, so that the dataset's existence can be discovered by others through its metadata, and access requested and granted as and when appropriate or permitted. When data are exceptionally sensitive, contact Faculty Research Support to discuss options.

### 8.2 Selection Criteria for Data Publication and Archiving

As a general rule, the raw research data and derived research data (processed data) used for a publication are archived. Sometimes one or more intermediate stages of data processing are also worthwhile preserving, for instance when they can be reused more easily than the actual source data or when effort is needed to create

them. Not *all* data and digital material associated with a publication merit long-term archiving. Ask yourself the following questions when considering if the data should or should not be archived:

- a) Are they really research data? [Files like presentation slides are not considered as data and probably are not needed for long-term preservation.]
- b) Are the data useful for future research?
- c) Are the data already archived as part of another project, or with a publication?
- d) Are the data directly relevant for your publication(s)?
- e) Are the data unique (impossible to recreate)?
- f) Are the data valuable (e.g., in terms of transparency, re-use, quality, originality, size, possibility to combine them with other data, production costs, or innovative nature)?
- g) Are there any obligations for long-term storage?
- h) Are the data subject to intellectual property rights or any other publishing restrictions?
- i) Are the data subject to privacy limitations, such as sensitive data, limitations to long-term archiving from a providing party, limitations following from a collaboration, etc.?
- j) If long-term preservation is chosen for the data, is the chosen infrastructure adapted to their characteristics (estimated cost, size, desired accessibility during preservation, etc.)?

### 8.3 Preferred / Certified Repositories

Research data should be deposited in a trusted repository (according to the Research Data Alliance's TRUST Principles for Trustworthy Data Repositories, ideally with CoreTrustSeal<sup>19</sup> or Nestor Seal (DIN 31644)<sup>20</sup> certification or meeting ISO 16363 standards). Researchers in the Faculty are free to choose a repository that best suits their project, but as a default, they are encouraged to use the Data Station Archaeology at the Dutch national institute for Data Archiving and Networked Services (DANS), which is an institute of the Royal Netherlands Academy of Arts and Sciences (KNAW) and the Dutch Research Council (NWO).

In accordance with protocol 4010 Depotbeheer (Depot Management) of the Dutch Archaeology Quality Standard (KNA), all researchers doing archaeological fieldwork in the Netherlands are formally obliged to deposit their data in the DANS Data Station Archaeology.

Other CoreTrustSeal-certified archaeology-specific repositories include The Digital Archaeological Record (tDAR) in the United States of America and Archaeology Data Service in the United Kingdom. Another popular, although not certified, option is Zenodo, the European OpenAIRE program's general-purpose open repository that is operated by CERN (The European Organization for Nuclear Research).

Note: under GDPR, personal data must be stored within the European Economic Area (EEA). If you are collecting any personal data, you must check whether your repository is hosted or maintains a server in the EEA.

### 8.4 Choosing a Usage License

Published research data should come with clear and accessible access conditions, and a data usage license. It is recommended to choose a usage license that makes data available to the widest possible audience, and allows the widest possible range of uses. As an example, CC-BY is the most open license that still requires the author to be referenced. It allows the user to redistribute, to create derivatives, such as a translation, and even use the publication for commercial activities, provided that appropriate credit is given to the author (BY) and that the user indicates whether the publication has been changed. Software developed for research or as a research output should have a software-specific usage license.

### 8.5 Data Access Protocol for Restricted Datasets

If and when a researcher determines that all or part of their research data should be published in a data repository under restricted access, the researcher is obliged to develop a **Data Access Protocol (DAP)** that contains all of the necessary information that will be needed for the Policy Officer or Research to process access requests. The DAP must then be archived in the Research Support Office with the final version of the project DMP. For all employees of the Faculty, it is highly recommended that the Policy Officer of Research, with the

---

<sup>19</sup> Check the list of CoreTrustSeal-certified repositories: <https://amt.coretrustseal.org/certificates>

<sup>20</sup> Check the list of Nestor Seal-certified repositories:

[https://www.langzeitarchivierung.de/Webs/nestor/EN/Zertifizierung/nestor\\_Siegel/siegel.html](https://www.langzeitarchivierung.de/Webs/nestor/EN/Zertifizierung/nestor_Siegel/siegel.html)

contact [researchsupport@arch.leidenuniv.nl](mailto:researchsupport@arch.leidenuniv.nl), be identified as the main point of contact for all such data access requests when depositing your research data as restricted access. Information on how to write a DAP and an accompanying DAP template are available in the [Guidebook Depositing Restricted Access in the DANS Data Stations](#) and can be used by researchers no matter where restricted access data are deposited.

## 8.6 Registering Published Research Data with LUCRIS

Upon the publication/deposition of research data, datasets, databases, or software, the Principal Investigator or Researcher is obliged to register that published data using the Leiden University Current Research Information System (LUCRIS). This should be conducted even when that data/software accompanies a publication that is also registered with LUCRIS. An exception to this would be if those data are only published as supplementary material to the publication and therefore the data and the publication share the same DOI. For additional information or guidance, email the [Policy Officer of Open Access](#).

## 9. Research Data Not Underlying a Publication

### 9.1 Archiving Data Not Underlying Publications

The Faculty encourages research data not underlying a publication to be archived or published in a trusted repository because some unpublished data may be worth preserving long-term. Possible appraisal criteria for unpublished data include:

- Are the data unpublished because it was produced during a pilot study, and/or because of an unexpected problem during data collection or analysis? If so, is it useful to document them / keep a record of them for future research?
- Are the data unique?
- Are the data (potentially) reusable?
- Would it cost a considerable amount of time/money to reproduce the data?
- Are there any obligations to preserve the data long-term (e.g., funder requirements)? [In principle, the University requires that data produced during funded research are archived for at least 10 years after the completion of a research project.]

If the answer to any of these questions is “Yes”, the researcher is encouraged to deposit the data in a trusted repository. Data Stewards can support this process.

### 9.2 Archiving Data Underlying BA, MA, and RMA Theses

As stated in §2, this protocol does not apply to BA, MA, or RMA students unless their research results in an academic publication (in which case the recommendations given in the previous sections apply, including the need to have received prior approval of the Ethic Committee, if required [see §6.8.1]). The minimal retention period of 10 years (see §11) likewise does not apply to this group, although it is advisable for data underlying a thesis to be retained, and made available to examiners on request, until at least one month after graduation. However, many students do create or collect original data in the course of writing their theses and may wish to preserve it.

If the data's size and format suit it, the data can be included in full as appendices to the thesis<sup>21</sup> and so be archived along with the manuscript in the [Leiden University Student Repository](#). Each student is required to determine—in consultation with their thesis supervisor(s)—whether their thesis (and the data underlying the thesis) will be made openly accessible or under a full/partial embargo within the Student Repository when they upload their thesis via the Graduation form. If the thesis (and the data underlying the thesis) will be made openly available, the [explicit written permission](#) of the supervisor(s) must be obtained.

If it is not practical to include within appendices the data underlying the thesis, the data may be appraised by the thesis supervisor(s) to assess whether the data and their documentation are of high enough quality to be archived in the DANS Data Station Archaeology or another repository. If this option is selected, the associated DOI associated with that data should be included in the student's thesis manuscript.

---

<sup>21</sup> [Guidelines for \[Theses and\] Papers in the BA, MA and RMA Programs](#), Faculty of Archaeology (September 2025 edition).

The student author and thesis supervisor(s) are jointly responsible for ensuring that archived data do not contain any personal data. When uncertainty arises whether something classifies as personal data, a Privacy Officer must be consulted. See §6.8.2 on Research Data Privacy.

## 10. Archiving Legacy Data

Legacy data refers to information that are stored in outdated or obsolete systems, formats, or technologies that are often difficult to access. Their provenance and current ownership may be unknown. This protocol does not (yet) prescribe any particular way of managing legacy data, but scientific and support staff are encouraged to identify and appraise legacy data when they find them, and to notify the [Faculty Data Steward](#) for further assistance.

### 10.1 Preparing for End-of-Contract or Retirement

At least 6 months prior to retirement or end-of-contract, researchers leaving the Faculty (including emeriti) are urged to assess their research data and enact a data management plan that includes: a) an explicit written agreement with management staff about what should happen to their legacy data, and b) the production of metadata that sufficiently describe their legacy data such that whoever assumes responsibility for them can understand and manage them. A detailed inventory of the legacy research data that is to be retained within the Faculty should be included with the data management plan.

### 10.2 Preserving Non-Digital Data

The storage and preservation of non-digital data – if any – is organized at the Department level. Researchers who are unsure what to do with their non-digital data at the end of the research project, or their career, are encouraged to contact the Faculty Data Steward to appraise the material and discuss options for safeguarding. If needed, the Faculty Data Steward will then seek the advice of [Archive Management](#) and the respective Department Head to determine a course of action for the long-term preservation of these non-digital data.

### 10.3 Archiving a Personal Non-Digital Data Collection

Researchers with an outstanding career scholarship record, and/or whose personal collection of non-digital data (e.g., notebooks, letters, sketches, rare books) can be considered to have (scientific-) historic value, may be able to donate their collection to the Special Collections department of the University Library (UBL). To inquire, please contact [Special Collections](#). Even if the collection cannot be re-homed with the UBL, it may well be relevant to the acquisition mandate of another foundation, library, or archive. In addition, Digital Scholarship Librarians at UBL may be able to assist you in digitizing (parts of) your collection, or transforming your data into a searchable archive or database (as in [this example](#)).

## 11. Retention Periods

At Leiden University, the default *minimal* retention period for research data is 10 years after the publication related to the data appeared.<sup>22</sup> The archiving period can be longer, depending on legal requirements, discipline-specific standards, and the intended purpose(s) of archiving the data. For archaeology and cultural heritage the retention period of research data is in principle indefinitely. When no particular restrictions apply, a dataset will commonly be archived without a maximum retention period; however, if a maximum retention period applies, there is an obligation to destroy the data after the expiry date. Destruction must be done properly, in accordance with archive law and regulations<sup>23</sup>; please contact [Archive Management](#) in the Administrative Shared Service Centre (ASSC) for support.

When the research data include personal data, the GDPR principle of data minimization<sup>24</sup> must be applied as soon as possible. That is, the data controller (in this case, the researcher) should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. In accordance with the

---

<sup>22</sup> Leiden University [Data Management Regulation](#)– version 1.0, 7-12-2021: §14.

<sup>23</sup> [Archiefwet 1995](#) [Archives Act 1995] (Ministerie van Onderwijs, Cultuur en Wetenschap 2022); [Regeling Archiefbeheer Universiteit Leiden](#) [Leiden University Archive Management Regulation] (College van Bestuur, Universiteit Leiden 2011).

<sup>24</sup> [General Data Protection Regulation](#) (Regulation (EU) 2016/679 of the European Parliament), art. 5(1)c.

principle of storage limitation,<sup>25</sup> they should also retain the data only for as long as is necessary to fulfil that specified purpose. Directly identifiable personal data such as contact information, signed consent forms, etc. may be stored separately from the main dataset for a *maximum* of 10 years, after which they must be destroyed. Note that merely deleting a file from a storage space often does not qualify as destroying it. An official declaration of destruction must be obtained from [Archive Management](#) to provide legal proof that all confidential data and associated physical records have been securely destroyed and are irretrievable.<sup>26</sup> Please contact the Research Support Office for additional information.

## Section: Roles and Responsibilities

### 12. Responsibilities

#### 12.01 Executive Board

The Executive Board is responsible for:

- a) Establishing the university-wide policy framework for RDM (at present: RDM2021) and evaluating these on a regular basis.
- b) Providing adequate central facilities and support to facilitate responsible RDM.
- c) Monitoring compliance with the University RDM Regulations on a regular basis.

#### 12.02 Faculty Board

The Faculty Board is responsible for:

- a) Providing the means and support for the elaboration, implementation, review, and regular evaluation of the Faculty RDM Protocol.
- b) Deciding on Faculty policy with regard to matters that are underspecified in University policy (for example, research data collected by students for their thesis).
- c) Providing adequate resources and support to allow for the implementation of the Faculty RDM Protocol and, in so doing, to meet University and funder requirements with regards to data management, privacy compliance, and ethics review.

#### 12.03 Executive Director of Research

The Executive Director of Research (accountable to the Faculty Board) is responsible for:

- a) Managing RDM practice and implementation throughout the Faculty.
- b) Advising the Faculty Board with respect to RDM practice.
- c) Presenting to the Faculty Board all revisions made to the Faculty RDM Protocol to seek their approval.
- d) Fostering (together with the policy officers of Research and Research Data) recognition and awareness of responsible RDM practice within the Faculty.
- e) Ensuring that review and evaluation of the Faculty RDM Protocol is scheduled at least once every two years, or whenever revisions are needed to remain compliant with any governing regulations and policies.
- f) Delegating or, if necessary, mandating RDM responsibilities to staff members and/or researchers on the Faculty level.
- g) Making final decisions with regards to research data produced within the Faculty (if the appropriate Principle Investigator and/or Department Head are not able), such as decisions about data access,

---

<sup>25</sup> [General Data Protection Regulation](#) (Regulation (EU) 2016/679 of the European Parliament), art. 5(1)e.

<sup>26</sup> [Regeling Archiefbeheer Universiteit Leiden](#) [Leiden University Archive Management Regulation] (College van Bestuur, Universiteit Leiden 2011), art. 8.

deletion/destruction of data, data auditing, etc. Such arrangements can be dependent on the development of University-wide and/or Faculty-wide solutions.

- h) Classifying research data as confidential (in consultation with the Faculty Board) if and when they deem that data to be harmful to the University and/or its stakeholders (see §3.3.7). At the end of the research project, the Executive Director of Research is responsible for guaranteeing that the confidential research data are properly destroyed.
- i) Making decisions (together with the concerned Department Head) regarding the transference of RDM responsibilities of the Principal Investigator (PI) to an appropriate staff member in the instance where a PI has left, retired, or is no longer present for other reasons.

#### 12.04 Policy Officer of Research

The Policy Officer of Research (accountable to the Executive Director of Research) is responsible for:

- a) RDM practice, in general, and policy development at the Faculty level.
- b) Executing the implementation of the Faculty RDM Protocol.
- c) Reviewing and regularly revising the Faculty RDM Protocol together with the Policy Officer of Research Data.
- d) Evaluating the Faculty RDM Protocol for relevance and adequacy at least once every two years, or whenever revisions are needed to remain compliant with any governing regulations and policies.
- e) Connecting researchers to relevant second-line support such as legal.
- f) Responding to and reviewing requests to access Faculty-produced research data that have been deposited as restricted access or locked with data repositories (such as the DANS Data Station Archaeology) as detailed in §8.5. Such requests are to be reviewed in accordance with the terms outlined in the associated Data Access Protocol (DAP) provided by the Principle Investigator responsible for the deposition of the restricted access data. If the Principle Investigator is no longer employed by the Faculty and is not accessible for consultation, recommendations are given to the Executive Director of Research who then makes the final decision to grant or deny access.
- g) Determining if research data may need to be marked as confidential due to their potential to harm the University and/or its stakeholders (see §3.3.7). Upon the identification of potentially harmful data generation, the Policy Officer of Research is obliged inform the Executive Director of Research of the proposed generation of research data that may need to be marked as confidential.

#### 12.05 Policy Officer of Research Data (Faculty Data Steward)

The Policy Officer of Research Data, also known as the Faculty Data Steward, (accountable to the Policy Officer of Research and the Executive Director of Research) is responsible for:

- a) Developing, reviewing, and revising the Faculty RDM Protocol in coordination with the Policy Officer of Research.
- b) Consulting researchers in RDM practices and on DMP development, unless that DMP is of their own research (i.e., in instances where the Data Steward is also a researcher).
- c) Providing feedback to DMPs and Data Management sections in grant proposals.
- d) Reviewing DMPs following submission to the Faculty DMP Repository (in SharePoint).
- e) Making sure RDM practice is generally compliant with relevant regulations.
- f) Pointing the Researcher to approved storage solutions and tools.
- g) Archiving project documentation including deleting documents after the retention period.
- h) Monitoring the deposition of datasets.
- i) Data curation for the Faculty data repository and checking of publication package structure and content.
- j) Raising awareness of RDM best practices within the Faculty.

- k) Developing and maintaining Faculty-specific RDM training and educational resources in complement to training and education provided by the Faculty and the Centre for Digital Scholarship (CDS).
- l) Choosing, developing, and maintaining Faculty-specific metadata standards and file naming and structuring conventions based on domain-specific standards, if available.
- m) Carrying out RDM tasks delegated by the Policy Officer of Research and/or the Executive Director of Research and reporting accordingly.

#### 12.06 Department Head

The Department Head (accountable to the Dean of the Faculty and the Executive Director of Research) is responsible for:

- a) RDM practice, in general, on the Department level (informed by the Faculty Data Steward).
- b) Facilitating the dissemination of information regarding RDM within the Department.
- c) Holding all Principle Investigators, Supervisors, Researchers, and research staff within the Department accountable to the Faculty RDM Protocol.
- d) Delegating or, if necessary, mandating RDM responsibilities to staff members and/or researchers on the Department level.
- e) Making final decisions (if the associated Principle Investigator is not able) with regards to research data produced within the Department, such as decisions about data access, deletion/destruction of data, data auditing, etc. Such arrangements can be dependent on the development of University-wide and/or Faculty-wide solutions.

#### 12.07 Principal Investigator

Principal Investigator (accountable to their supervisor) is responsible for:

- a) Developing and maintaining RDM procedures for their research project and/or research group in consultation with the Faculty Data Steward.
- b) Creating and developing a project DMP, updating the DMP as and when needed, and ensuring that all project collaborators are aware of and adhere to the most recent version of the DMP.
- c) Ensuring clarity about data ownership and RDM responsibilities from the beginning of the research project, and that these are documented in any associated DMP and/or collaboration agreement.
- d) Informing their research group members about RDM policies and procedures, providing means for their implementation, and monitoring compliance to all relevant regulations.
- e) Reviewing and approving all DMPs of their research group prior to submission to granting agencies and/or to be filed with the Faculty Data Steward.
- f) Ensuring that all project research data are stored on internally controlled and secured storage spaces (such as the MS SharePoint, SURF Research Drive, or Yoda) and not on personal storage space (such as MS OneDrive or SURFdrive).
- g) Ensuring that they and at least one other staff member always have access to all research (meta)data/software of their research group. The PI should either be in charge of the management of project research data storage or they should delegate this responsibility to a clearly identified project researcher.
- h) Archiving the research project DMP(s), and overseeing the appropriate long-term storage or archiving of the research data and project documentation at the end of the research project.
- i) Registering or delegating responsibility to register with LUCRIS all published (meta)data/software produced from a research project.
- j) Transferring RDM responsibilities to an appropriate staff member upon leaving or retiring as directed by the Department Head or Executive Director of Research and in consultation with the Faculty Data Steward.

- k) Assuming responsibility with the associated Supervisors, if relevant, for curatorial decisions (e.g., the deletion or migration of data) for all research data retained by the Faculty after a project researcher leaves Leiden University.

#### 12.08 Supervisors

Supervisors (accountable to the Department Head and the Executive Director of Research) are responsible for:

- a) Ensuring that staff, students, and guest researchers under their supervision have access to the necessary knowledge, skills, and resources to manage their research data appropriately.
- b) Advising staff, students, and guest researchers under their supervision in RDM planning and ethics review applications.
- c) Monitoring that their supervisees are carrying out their research along the lines set out in their DMP and ethics review documentation.
- d) Reviewing and evaluating the compliance and effectiveness of the RDM practices of the staff and students under their supervision during yearly Performance and Development Interview.
- e) Ensuring that the ethics committee and Faculty Data Steward are appropriately made aware of any significant changes in a supervisee's DMP.
- f) Verifying that appropriate decisions are made and actions realized relating to the retention, transference of ownership, or destruction of supervisees' research data held in the University's storage environments near their end of contract and/or before supervisees leave Leiden University.
- g) Assuming responsibility with the associated Principal Investigator, if relevant, for curatorial decisions (e.g., the deletion or migration of data) for all research data retained by the Faculty after a supervisee/researcher leaves Leiden University.

#### 12.09 Project, Facility, or Laboratory Managers

RDM tasks may be delegated to Project, Facility, and/or Laboratory Managers (accountable to their supervisor and the Department Head). In these cases, they are responsible for:

- a) Developing, maintaining, disseminating, and facilitating the implementation of RDM procedures for their project, facility, or laboratory in consultation with their supervisor and the Faculty Data Steward.
- b) Being aware of where their team members store their files, and making sure that, if necessary, access to and/or stewardship of their data is transferred to them (or another appropriate staff member such as the Principle Investigator or Supervisor) at the end of a research project or an employment term.

#### 12.10 The Researcher

The researcher (accountable to the Principle Investigator and/or Supervisor) is responsible for:

- a) Familiarising themselves and complying with the relevant data management, record-keeping, open data, and retention requirements of research funders, sponsors, publishers, and other relevant external stakeholders, as well as the relevant legal, ethical, and regulatory frameworks governing the processing of personal data and sensitive research data.
- b) Carrying out their research and RDM practice according to the steps described throughout this protocol.
- c) Following the RDM procedures of the research group and those of any research facilities or laboratories in which they conduct research.
- d) Drawing up, updating, submitting, and archiving DMPs for their research, according to the terms outlined in the protocol, and then managing research (meta)data/software accordingly. All research can benefit from RDM planning, and researchers are obligated to create a DMP before starting any research project.
- e) Ensuring DMPs are approved by the Principal Investigator and/or Supervisor prior submission to the Faculty DMP Repository.

- f) Making appropriate decisions relating to the retention, transference of ownership, or destruction of research data held in the University's storage environments if/when they leave Leiden University. Responsibility for curatorial decisions thereafter (e.g., the deletion or migration of data) lies with the Principal Investigator or Supervisor, and ultimately with the Department Head and/or Executive Director of Research.

## 13. Where to Find Support

### 13.1 Faculty Support Staff

- Data Steward / Policy Officer of Research Data: Adam K. Benfer ([rdm@arch.leidenuniv.nl](mailto:rdm@arch.leidenuniv.nl))
- Policy Officer of Research / Research Support Office (RSO) Coordinator: Jimmy Mans ([researchsupport@arch.leidenuniv.nl](mailto:researchsupport@arch.leidenuniv.nl))
- Privacy Officer: Max van Arnhem ([privacy@bb.leidenuniv.nl](mailto:privacy@bb.leidenuniv.nl))
- Information Manager/ Security Officer/ ICT Coordinator: Jasper Kanbier ([helpdesk@arch.leidenuniv.nl](mailto:helpdesk@arch.leidenuniv.nl))
- Graduate School Coordinator/ Policy Officer of Open Access: Gabi Perhaj ([graduateschool@arch.leidenuniv.nl](mailto:graduateschool@arch.leidenuniv.nl) / [lucris@arch.leidenuniv.nl](mailto:lucris@arch.leidenuniv.nl))
- Ethics Committee Secretary: Myrte Vos [at Faculty of Humanities] ([ethics@hum.leidenuniv.nl](mailto:ethics@hum.leidenuniv.nl))

### 13.2 Central Support

- [Research Support Portal](#)
- Leiden University Libraries' (UBL) [Centre for Digital Scholarship \(CDS\)](#):
  - [Copyright Information Office](#): [auteursrecht@library.leidenuniv.nl](mailto:auteursrecht@library.leidenuniv.nl)
  - [Research Data Management](#): [datamanagement@library.leidenuniv.nl](mailto:datamanagement@library.leidenuniv.nl)
  - [Research Software & Data Engineering](#)
  - [Open Science and Open Access](#): [openaccess@library.leidenuniv.nl](mailto:openaccess@library.leidenuniv.nl)
- [Research IT Support](#): [rits@issc.leidenuniv.nl](mailto:rits@issc.leidenuniv.nl)
- [Privacy Service Point](#): [privacy@bb.leidenuniv.nl](mailto:privacy@bb.leidenuniv.nl)
- [Security Office SharePoint \[Dutch only\]](#): [security@bb.leidenuniv.nl](mailto:security@bb.leidenuniv.nl)
- [Grant Development Office](#): [grants@bb.leidenuniv.nl](mailto:grants@bb.leidenuniv.nl)
- [Knowledge Exchange Office \[for legal advice\]](#): [luresearchcontracts@luris.nl](mailto:luresearchcontracts@luris.nl)
- [Archive Management office](#): [dia@assc.leidenuniv.nl](mailto:dia@assc.leidenuniv.nl)
- [Knowledge Security \[for International Collaboration\] Advice Desk](#): [adviespuntkv@bb.leidenuniv.nl](mailto:adviespuntkv@bb.leidenuniv.nl)

### 13.3 Training and Information

For training on research data management, please sign up for the Centre for Digital Scholarship's regular workshops and the obligatory research data management workshop for PhD researchers in the Faculty. These also include support in writing a DMP.

## 14. Reporting Incidents

### 14.1 Data Loss or Corruption

In the case of loss or corruption of data, the researcher is obligated to immediately report this to the Research Support Office (RSO). This is not necessary if a very recent backup was available - unless personal or sensitive data are involved. In the latter case, a report always needs to be made.

### 14.2 Data Leaks

When personal or sensitive data are compromised or lost, this problem has to be reported to the ISSC Helpdesk to start the data breach procedure. The RSO should be informed at the same time.

## 15. Procedures for this Data Protocol

This RDM protocol takes effect as of February 12, 2026, and does not apply retroactively. At this time, all parties that have responsibilities stated in this Protocol are expected to be aware of this Protocol. The RDM Protocol is

evaluated and revised at least once every two years, or whenever revisions are needed to remain compliant with any governing regulations and policies.

The RDM Protocol was approved by the Faculty Board on February 12, 2026.

## Appendix 1: Relevant Legislation and Agreements

A detailed list of the relevant legislations, whether they apply to all scientific disciplines (elaborating on RDM2021, §2) or are specific to the Faculty, is given below:

### 1.1 National Legislations and Guidelines

- Archiefwet 1995 [Archives Act 1995] (Ministerie van Onderwijs, Cultuur en Wetenschap 2022) [\[NL\]](#)
- Auteurswet [Copyright Law] (Ministerie van Justitie 2025) [\[NL\]](#)
- Code of Ethics in the Social and Behavioural Sciences Involving Human Participants (National Ethics Council for Social and Behavioural Sciences 2018) [\[EN/NL\]](#)
- Guideline for the Archiving of Academic Research for Faculties of Behavioural and Social Sciences in the Netherlands (Deans of Social Sciences in the Netherlands 2022) [\[EN\]](#)
- Handleiding Algemene verordening Gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming [General Data Protection Regulation Manual and Implementation Act for the General Data Protection Regulation] (Ministerie van Justitie en Veiligheid 2023) [\[NL\]](#)
- Kwaliteitsnorm Nederlandse Archeologie [Dutch Archaeology Quality Standard] (College voor de Archeologische Kwaliteit 2024) [\[NL\]](#)
- Netherlands Code of Conduct for Research Integrity (NWO 2018) [\[EN\]](#)[\[NL\]](#)
- Wet op het Hoger onderwijs en Wetenschappelijk onderzoek [Higher Education and Scientific Research Act] (Ministerie van Onderwijs, Cultuur en Wetenschap 2023) [\[NL\]](#)

### 1.2 University Guidelines

- Leiden University Archive Management Regulation [\[NL\]](#)
- Leiden University Data Management Regulation [\[EN\]](#)[\[NL\]](#)
- Leiden University Employer Copyright Regulations [\[EN\]](#)[\[NL\]](#)
- Leiden University policy on privacy and information security [\[EN\]](#)[\[NL\]](#)
- Leiden University Policy Framework for Knowledge Security [\[NL\]](#)

### 1.3 Faculty-Specific Guidelines and Protocols

- Co-authorship Considerations and Guidelines, Faculty of Archaeology [\[EN\]](#)
- Code of Conduct for Fieldwork in the Faculty of Archaeology [\[EN\]](#)
- Regulation of the Ethics Committee of the Faculty of Humanities and the Faculty of Archaeology [\[EN\]](#)[\[NL\]](#)
- Research Data Management in Archaeology [\[EN\]](#)

### 1.4 International

- Ethics in Social Science and Humanities (European Commission 2021) [\[EN\]](#)
- General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament) [\[EN\]](#)
- Practical Guide to the International Alignment of Research Data Management (Science Europe 2021) [\[EN\]](#)
- Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity (United Nations 2010) [\[EN\]](#) [\[NL\]](#)
- United Nations Declaration on the Rights of Indigenous People (United Nations 2007) [\[EN\]](#)
- Handbook of Data Protection Laws of the World: An Overview of Key Privacy and Data Protection Laws Across More Than 160 Jurisdictions (DLA Piper 2025) [\[EN\]](#)
- UNESCO Database of National Cultural Heritage Laws [\[EN\]](#)

### 1.5 Other Guidelines

- The CARE Principles for Indigenous Data Governance [\[EN\]](#)
- The FAIR Principles for Scientific Data Management and Stewardship [\[EN\]](#)
- The TRUST Principles for Digital Repositories [\[EN\]](#)