Research Data Policy Plan

Version: 3.0
In effect as of: 1 September 2022

Center for Religious Studies
Faculty of Theology and Religious studies

Table of Contents

1. Introduction

This document outlines the general policy relating to research data management in the Faculty of Theology and Religious Studies, and it sets out the specific procedures expected of all staff and students based in the Faculty.

The general Faculty's attitude regarding to data management is that we accept that our staff has a professional competence and autonomy. They can assess situations carefully and act according to an 'everyday ethics': in each case they can decide what is the best course of action.

At the same time, it is also the Faculty's social and legal responsibility to provide guidelines, to offer support to our staff and students, to train them in data management and to maintain oversight of all data processing activities.

This protocol is based on the UG Research Data Policy 2021 that sets out university-wide standards and responsibilities for data management.[1] It is offers more discipline-specific and practical guidelines for treating data.

With this protocol, the faculty aims to enhance both (1) the transparency of research and (2) the safekeeping and securing of information.

2. Governance and standing of this document

This research data management (RDM) policy document was developed in response the new UG Research Data Policy 2021. This document was developed by the faculty's research policy advisor, and the privacy and security coordinator and has subsequently been approved by the faculty board. This document will be revised from time to time and is subject to changes in the various regulations that underpin it. It also needs to be read alongside the following documents:

- the Faculty's policy and procedures on Research Ethics
- the 2020 University of Groningen Code of Conduct on Integrity
- the 2018 Netherlands Code of Conduct for Research Integrity
- the European General Data Protection Regulation
- Ethics and data protection (2018)
- the University of Groningen Research Data Policy (2021)
- the 'Practical Guide to the International Alignment of Research Data Management' by Science Europe (2021)

3. Scope

The subject matter of this policy is the proper management of all data processed in research activities at the Faculty of Theology and Religious Studies. and research data processed in collaboration with national and international research partners.

This plan also covers research data processed by students enrolled in our Bachelor's and Master's degree programmes. However, given the differences between staff members and students the Faculty will produce specific instruction for students, in line with this policy.

The scope of this plan hinges on a definition of 'research data' that does justice to the research performed at the Faculty of Theology and Religious Studies. The UG Research Data Policy

[1] https://www.rug.nl/digital-competence-centre/ug-research-data-policy-2021.pdf

defines research data as “codified and recorded facts and observations ensuing from scientific research”. This first of all seems to suggests that data are literally ‘given’, and ‘empirical’ and ‘objective’ by nature, and that they can exist independently of the activities of the observer.

Data in the field of Theology and Religious Studies, on the other hand, deals with interpretations, meanings, or cultural and religious practices. ‘Raw data’ in the humanities are an effect of an interpretive processes, and a result of a relationship of trust between the researcher and the participants. In some cases the data are produced by actively participating in rituals and practices. In other words, instead of given, it might be more appropriate to define ‘data’ as ‘taken’ rather than as ‘given’.[2]

Data within this field can come in all sorts of different shapes and sizes. In many cases, researchers perform literature research in publicly available resources. In the fields of spiritual care, anthropology, sociology and psychology of religion, more ‘qualitative’ data is being processed. Our researchers take field notes, make recordings, use manuscripts, process social media feeds or they might use statistical databases. Even notes, analyses or reports on literature research could count as research data. [3]

It will be too challenging to provide an exhaustive list of what counts as data. This document therefore starts by defining data as all materials and assets collected, generated and used during all stages of the research cycle, and which need proper management in order to be protected against accidental or unlawful destruction, loss, alteration, or unauthorised disclosure. To this it needs to be added that a research project should in principle be able to be reconstructed, and therefore the data should be available upon request.

Although this policy devotes special attention to personal data, non-personal data also fall within its scope.

Lastly, ‘data’ should mainly be taken as ‘digitalised data’, but researchers may also store non-digitalised data carriers, in e.g. paper format (such as questionnaires), or audio-tapes. This policy will mainly focus on digital data.

4. **Principles of data management**

There are several key overarching principles that govern research at the University of Groningen and at universities in general:

1. All research is to be undertaken according to relevant legislation, the requirements of ethically responsible research[4], such as informed consent, academic integrity[5], the arrangements set out in cooperation agreements, and the research conditions of funders.
2. When personal data are processed in research, then these must be handled in a way that meets the European General Data Protection Regulation (GDPR). In particular, this entails the requirement to demonstrate that appropriate technical and organizational measures to achieve privacy by design are in place.
3. Where feasible and ethically appropriate, researchers will make their data FAIR.
4. Research methodologies, experimental design, data, data analysis, statistics, results and interpretations should be subject to peer review and scrutiny, and all researchers should be able to substantiate their choices, and be able to provide access for validation

[2] Drucker, J. (2011) proposes that the term ‘capta’ is more fitting to the Humanities. See: Humanities Approaches to Graphical Display. Digital Humanities Quarterly 005, no. 1. http://www.digitalhumanities.org/dhq/vol/5/1/000091/000091.html

[3] See De Koning et al., ‘Guidelines for anthropological research: Data management, ethics, and integrity’, in: *Ethnography* (2019), Vol. 20(2) 170–174.

[4] https://www.rug.nl/about-ug/policy-and-strategy/research-ethics/

[5] https://www.universiteitenvannederland.nl/wetenschappelijke_integriteit.html

of the integrity of the data. Also, the software and scripts that are developed for the collection, analysing or representation of data are relevant in this context.

5. When conflicts arise between this document, and one or several of the other guidelines mentioned in section 2, or when ethical dilemmas arise, it is expected that assistance is sought from the supervisor, the Research Ethics Committee, or the Faculty Board.
6. We expect that our researchers, PhD-students and students adopt a 'comply or explain' attitude. Researchers will be expected to comply with the expectations described in this document. In cases where there is a need to deviate, it will be expected that an explanation can be provided, and that appropriate technical and organizational measures aimed to protect the data are demonstrably in place.

5. Personal data and data protection

5.1 The GDPR and research data

Most research at our faculty uses publicly available resources, such as manuscripts or literature. However, in some cases researchers process personal data in their research.

Since May 2018, all member states of the European Economic Area share the same data protection law: the General Data Protection Regulation (GDPR). This law governs the processing of personal data both inside and outside the EU/EEA when this is done by organisations based in one of the member states. This law also applies to research activities by universities, even when these take place in non-member states.

Personal data in the GDPR are defined as "any information relating to an identified or identifiable natural person" (Art. 4.1). A 'natural' person means a living person. In the GDPR, there is no distinction between public and private/confidential data, only between personal and non-personal data. All personal data should be treated as confidential.

Examples of 'identifiers' are names, an identification number, contact details, location data, IP-addresses, ethnicity, religious identity, or a combination of data that allows for a person to be identified as a unique individual. 'Processing' should be understood as any operation with data: gathering, viewing, analyzing, storing, sharing etc.

The GDPR sets constraints to what is possible with personal data. However, there are specific derogations for researchers when data are processed for historical, statistical or scientific purposes and the researcher can demonstrate compliance.

5.2 Accountability: demonstrate compliance

A central principle in the GDPR is 'accountability'. If you are planning to process personal data in your research, then you need to be able to demonstrate compliance with the GDPR.[6] This means that researchers are expected to design their research in such a way that the private lives of participants as well as their rights and freedoms are minimally impacted, and that researchers can show how this will be achieved.

We therefore expect researchers to anonymise data when possible, design their research in a privacy-friendly way, think about appropriate technical and organizational measures, register their research proposals in the tool provided by the Ethics Committee, create a data management plan and we expect them to seek feedback from the Ethics Committee on their proposal (see for a step by step procedure section 8).[7]

[6] See the factsheet of the European Data Protection Supervisor via https://edps.europa.eu/sites/edp/files/publication/18-12-11_factsheet3_documenting_data_processing_en.pdf (latest access: 24-11-2021).

[7] https://www.rug.nl/research/centre-for-religious-studies/research-ethics-committee?lang=en

Apart from a research data management plan, research involving living human beings may also require doing a Data Protection Impact Assessment (DPIA). A full DPIA report:

- maps the data privacy risks in the project;
- assesses these risks; and
- defines protection measures to eliminate or mitigate the risks.

Performing a DPIA is legally required when data processing activities are likely to 'result in a high risk to the rights and freedoms of natural persons '(art. 35 GDPR). In particular, these include large-scale processing of the 'special categories' of personal data such as ethnicity, religious and philosophical beliefs, automated processing of data, the use of new technologies, or systematic monitoring of publicly accessible areas.[8]

If a DPIA is required, then this should take place before data processing starts.

A DPIA can be supported by the Digital Competence Center and the Privacy and Security Coordinator. The process may be time-consuming. Researchers are therefore advised to contact the DCC as soon as possible (see section 20 on support).

If a DPIA has already been performed on a similar research project at our or at a different research university in the EU/EEA zone, then this can also be used as a point of reference, provided that the data protection measures set out are demonstrably applied by the researcher.

6. Informed consent

Although there are many aspects to ethical research, the concept of informed consent is fundamental. Informing research participants is also one of the duties in the GDPR.

6.1 Informing the research subject and obtaining consent

In principle, all research participants should be fully informed about all aspects of the research, including plans for the storage of data, and their informed consent has been obtained before their data is collected.

The researcher should also be able to demonstrate that they have genuinely obtained consent from their participants. The GDPR introduces a set of requirements of genuine consent, and there are also requirements to what information should be provided to the research subject. The Digital Competence Center provides a template and a checklist of all required items.[9]

Informed consent could take several forms. A common way would be to provide the subjects with an information sheet and a sheet that specified the various options for consent, including date and signatures of both research subject and researchers. Yet, there can be other possibilities to inform participants, for example using video materials, infographics or other visual support.

The information to be provided to the participants should be suited to the intended audiences. Participants have to be able to understand what they are consenting to. For people in vulnerable groups (e.g. children), tailor-made approaches may therefore need to be considered.

6.2 Informed consent and the special categories of data

[8] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

[9] https://www.rug.nl/digital-competence-centre/guides/data-privacy-and-protection

Special categories of data are data revealing information about:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data, biometric data for the purpose of uniquely identifying a natural person,
- health,
- person's sex life or sexual orientation.

These data can potentially be used to discriminate. Processing of special categories of personal data (e.g. information on health, religion, political views etc.) is therefore forbidden, except explicit consent has been given by the research participants. Based on the GDPR in Dutch law, the processing of special categories of data is also allowed when:

- it is necessary for the research purpose; and
- the processing is proportionate to the aim pursued; and
- the essence of the right to data protection are respected; and
- the controller provides suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects.

6.3 Informing the research subject without prior consent

There may be cases in which data is processed without prior consent of the research subjects (e.g. in the case of use of social media data, or by doing covert observations). When the personal data are provided to by a third party and the data subjects have not expressly consented to its use in research projects, they should be informed of the acquisition of the data and its intended use.

There are also exceptions in the GDPR to the obligation to inform participants for research purposes.[10] The researcher will still need to demonstrate that the exceptions are in fact applicable, and will regardless implement appropriate safeguards, including technical and organisational measures to achieve privacy by design and, make the information that should be provided to the data subjects, publicly available.

7. Use of social media data in research projects

Social media are ubiquitous today. They are readily available, can be used without training and make connecting to people easy. Social media also harbor vast amounts of user data and they can be used to uncover social relations between users. The apps are also usually cost efficient to use.

These factors make social media an interesting 'place' to explore untapped potential for research purposes. It is possible to efficiently recruit participants, evaluate behaviours, analyse expressions and discourse, or to study practices and rituals.

However, there are a couple of there are potential ethical and data protection risks involved in collecting data from social media that also deserve exploration and mitigation. Researchers have a duty to scrutinize the risks, understand them and demonstrably take appropriate data protection measures before utilizing social media apps and platforms for research purposes.

[10] The obligation in GDPR Art. 14 may not applicable when it requires a disproportionate effort (rec. 62) OR when the obligation is likely to render impossible OR seriously impair the achievement of the objectives of the processing.

It will not be possible to exhaustively list all potential ethical and legal hazards, but there are a couple of points to consider:

- The GDPR does not distinguish public from private data, but only personal from non-personal data. As a consequence, most of the social media data is defined as personally identifiable data under the GDPR, even if the personal data is published by the data subject himself or herself.

- Social media users themselves may also have expectations of a social media platform that do not match a binary public/private distinction, since many platforms offer gradual privacy settings.[11] They may also not be aware that the data they share can be publicly accessed since privacy controls may be tricky to use.

- It possible to data gather without knowledge and consent of the potential research participants. Researchers should carefully assess if and when they need to inform participants about the research, including the risks of participation. They also need to take into account whether this would require a disproportionate effort and come up with a strategy to handle this.

- Social media users often use pseudonym accounts. It may be hard to establish the identity of the users. There is a possibility that multiple people post items with the same account. This could potentially affect the quality of the data.

- The concept of 'identity' itself may also be contested. People may consider their online identity to be just as real as their legal identity. It is imaginable that an online identity suffers from negative consequences (such as reputation or economic damage) as a result of a breach in confidentiality.

- Social media platforms may set their own goals with their data processing activities, and use technologies that are difficult to comprehend by non-specialists. Researchers who use social media platforms to recruit participants should be aware that the social medium may gather and store data about any contact between researcher and participant, and monitor all activities on the platform, and that data processing is already taking place before consent is obtained.

The faculty's general attitude towards the use of social media data is that researchers who plan on using these data, should understand the risks involved and make a plan that should give due consideration to at least[12]:

a) the potential **risks and harms** that the research could harbor to social media users, especially when they are potentially vulnerable, such as is the case with children[13];
b) how potential research participants are **recruited**;
c) the question if **consent** is needed from the research participants;
d) which **information** should be provided to the research participants;
e) the **intentions and expectations** of the social media users; if they are likely to perceive their contributions to be public or private, their expectations about anonymity, and their expectations about research on their data;

[11] For example, LinkedIn offers the possibility to indicate who can see profile pictures: 'contacts', 'second and third degree contacts', 'only LinkedIn members', or 'everyone', i.e. being retrievable via search engines.

[12] Based on the document 'Ethics and data protection' section VII pg.12-14. This document "has been drafted by a panel of experts at the request of the European Commission (DG Research and Innovation) and aims at raising awareness in the scientific community, and in particular with beneficiaries of EU research and innovation projects. It does not constitute official EU guidance."

[13] A DPIA can help identify these risks in greater detail.

f) **the privacy policy and the terms and conditions** of the social media platform; if the intended use of the data complies with the terms and conditions for the use of the platform; how the social media company treats the data of users; the privacy settings of the platform;
g) **storing, sharing and archiving** of the social media data, in line with this policy;
h) Which **technical and organizational measures** are appropriate to mitigate the risks.

The Digital Competence Center has provided a checklist for the use of data gathered from social media. We expect that researchers use this checklist when designing a data management plan that involves the use of social media data and that they contact the Research Ethics Committee.

8. Planning data collection

In planning research and the methodology to be used, it is important to consider the ethical as well as practical implications of how the research is to be conducted and data collected and managed. Awareness of the requirements should influence the design of the methodology. The planning of the research must include the need to consider ethical issues and the requirements relating to data management.

8.1 Research data management plan

A research data management plan (RDMP) helps researchers reflecting on the kind of data that will be collected or produced, the facilities you need, how to safely store and manage the data, and how to make your data FAIR (Findable, Accessible, Interoperable and Reusable). Many funding bodies require an RDMP as part of a grant proposal.

8.2 Ethical assessment

As of 2020, the procedure for making a data management plan, registration of research and submitting a request for the Ethics Committee are integrated. Making a research data management plan is part of the assessment procedure of the Research Ethics Committee. It is expected that the faculty in the near future will make use of the Research Gateway tool developed by the faculty of Behavioral Sciences to register research proposals, but until then an intermediate tool will be offered. *Procedures may vary accordingly*. More information will be provided on the website of the Research Ethics Committee.

8.3 General procedure for academic staff

1. All researchers register their research proposal in the (provisional) registration tool provided by the faculty's Research Ethics Committee on their website.
2. Researchers follow the *full* procedure for ethical assessment in the following cases:
    a. when the research is conducted on living humans;
    b. when the research procedures might pose a danger to the researcher(s) and/or assistants;
    c. when the research objectives might cause a conflict of interest.
3. Approval by the ethics committee must be requested well in advance of the commencement of data collection. Data collection may not commence before the ethics committee has communicated its approval of the research to the applicant.
4. Requests for approval must be made through the registration portal or by email to ethicscommittee.ggw@rug.nl
5. At the request for approval, researchers will complete a questionnaire in which they reflect upon ethics, data protection and data management of their research (see Appendix 2). In addition, they submit their research plan and any informed consent forms or participant information forms they will be using.

6. Should approval by an ethics committee be a requirement for a research grant application, the researcher can submit only the grant application for preliminary approval. When the grant is awarded, the researcher should submit the documents stated in 8.3.5 for definitive approval by the ethics committee.
7. The ethics committee will inform the applicant of its decision within six weeks after the request was made.
8. The (revised) research data management plan is sent to the supervisor and Faculty Board along with the project budget.
9. After having obtained approval by the ethics committee, researchers store the completed questionnaire and letter of approval by the ethics committee on the Y-drive (Y:\staff\ggw\Datamanagement) and submit them for their annual R&O interviews.
10. The researcher will discuss the data management plan with the supervisor during their Results and Development (R&O) interview. If changes need to be made, a new version will be sent to the Faculty Board.
11. The CRS will perform sample checks on all data management plans. Data management is discussed once a year by the CRS based on a comparative analysis of all data management plans.

Temporary project researchers are also required to draw up a data management plan, and they are included in the R&O cycle. In research projects that involve several Faculty researchers (e.g. NWO, ERC), the project leader has final responsibility for the data management plan(s).

8.4 Procedure for PhD candidates

1. At the start of the PhD programme, the PhD candidate discusses the research proposal, data management plan and possible ethical issues, as well as the TSP with the main supervisor. The PhD candidate register the research proposal in the (provisional) registration tool provided by the faculty's Research Ethics Committee on their website.
2. The Phd candidate submits the TSP to the Director of the Graduate School. The TSP must be approved by the Director of the Graduate School before the research can take place.
3. PhD candidates follow the procedure for ethical assessment and request full approval by the ethics committee of their research in the following cases:
   a) when the research is conducted on living humans;
   b) when the research procedures might pose a danger to the researcher(s) and/or assistants;
   c) when the research objectives might cause a conflict of interest.
4. Approval by the ethics committee must be requested well in advance of the commencement of data collection. Data collection may not commence before the ethics committee has communicated its approval of the research to the applicant.
5. At the request for approval PhD candidates will complete a questionnaire in which they reflect upon ethics, data protection and data management of their research (see Appendix 2). In addition, they submit their research plan and any informed consent forms or participant information forms they will be using.
6. The ethics committee will inform the applicant of its decision within six weeks after the request was made.
7. After having obtained approval by the ethics committee, PhD candidates submit the completed questionnaire and letter of approval by the ethics committee for the go/no go interview. The supervisor of the PhD candidate stores these files on the Y-drive (Y:\staff\ggw\Datamanagement).
8. The PhD candidate then submits the approved data management plan and the TSP to the Faculty Board's Secretariat, who will store the documents in Hora Finita.
9. The data management plan will be discussed during the interim evaluation and updated if required. The new version will be stored in Hora Finita by the Faculty Board's Secretariat.

10. At the end of the PhD programme, the candidate must declare that the data have been stored on the Y drive.
11. External PhD students submit a data management plan as part of the admissions procedure for the Graduate School. The plan must be approved by the Director of the Graduate School.

9. Processing and storing data during research

Data is to be collected in an ethically responsible way. During the data collection process, there needs to be security of data already collected. For example, questionnaires should be securely stored. Audio or video recordings should be transferred to a password protected device as soon as possible. Initially data is likely to be re-identifiable, with the identification kept separate to actual data; however, it should be anonymised as soon as practical.

9.1 Storing during the research

All data generated during the research must be retained (e.g. audio and visual recordings, interviews, questionnaires, drawings, photographs, field notes, memos, codes, interview transcripts, SPSS data files).

In case of processing personal data: as a rule, the data package should never contain data that are not anonymized or pseudonimized[14]. In these cases, the data package should contain the first version of the data that can be anonymized or pseudonimized (for example, a transcript using pseudonyms in the case of audio recordings). The package will have to include information specifying where and how (and to whom) these original data are available.

Digital data must be stored on the University Workspace X or Y drive to ensure automatic and secure backups. The UWP can be accessed via a secure VPN connection. The formats used must be future-proof (see appendix 4.1).

Request extra storage capacity if there is more than 8 GB (X drive) or 100 GB (Y drive) of data by contacting the Faculty Demand Manager (see 'Support'). If more than 3 TB of capacity is required then a charge may apply. Make sure to include the cost item for this extra data storage capacity in the research budget. The Digital Competence Centre (dcc@rug.nl) can help to calculate the extra data management costs as part of a grant application.

Storing data on mobile devices is generally to be avoided. If you do, and if your data is not sensitive, create frequent back-ups at the very least and transfer data as much as possible to the UWP storage. If there is not another option available (e.g. there is no internet connection in the location where the research takes place), and the data is sensitive, then the device's harddrive should be encrypted, and the data should be stored on the UWP when this is possible.

Choosing external cloud services not managed by the UG (e.g. Dropbox, iCloud, OneDrive etc.) to store research data is also not recommended, especially when the data are personal or otherwise sensitive. Third party vendors may set their own goals that are not compatible with the University's policies on privacy and intellectual property rights. The UG has legal agreements with specific third party vendors that limit what vendors are allowed to do with the data.

Non-digitalized data, such as paper transcripts and questionnaires, or audio-tapes, need to be physically properly secured by using locked cabinets in a locked office.

[14] The difference between pseudonymized and anonymized data is the following: anonymization irreversibly destroys any way of identifying the data subject, while pseudonymization substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject.

9.2 Sharing data

The University of Groningen offers several secure ways to share and transport data through its own infrastructure or that of trusted partners:

- Y drive: data sharing with other University staff and students (100 GB).
- Unishare: a personal cloud service maintained by the UG. Unishare can be used to share data with colleagues from other universities (250 GB).
- SURFDrive: personal cloud service managed by SURF (the organization of CIT departments of Dutch Higher Education institutions. SURFDrive can also be used to share data with colleagues from other universities (500 GB).
- SURFfilesender: can be used to safely send files up to 1 TB. There is also the option of encryption and sending the recipient a key (up to 2 GB).

Google Drive can be used for collaboration and sharing files, but it is less suitable for processing research data, given the lack of a backup.

See the overview in appendix 2.

Contact the Digital Competence Centre (dcc@rug.nl) to discuss other situations involving data sharing with external parties (such as businesses). They can provide advice on capacity, security and legal requirements.

9.3 After the research

Once the research has been completed, the researcher is required to store the on the Y drive. Note that all data must be fully anonymised as soon as practical to do so.

The Secretariat of the Faculty Board reserves capacity on the Y drive for each researcher. Only the individual researcher (and the members of the research team, if they have authorization) has complete access to this capacity on the Y drive. The Director of the Graduate School (for PhD candidates) and the Faculty Dean (for academic staff) are authorized to access the data if there is sufficient reason to do so (only with read rights).

The researchers must also archive the data according to FAIR-principles, essentially making the data available to a wider audience for possible re-use. Archiving is usually done in a data repository.

This applies to:

- data on which the publication(s) is/are based, unless this data is fully accessible in public archives or databases
- data that is required to be archived by the funders of the research
- data that may be required for reuse by other parties (with the researcher's permission)

It is also recommended to archive unique data that can only be generated once and data that would be extremely costly (in money and/or time) to regenerate.

10. Publishing and Archiving

Data files that may be made public are stored in the data repository of DataverseNL. Publications are registered in Pure. Describe your dataset in Pure and link it to your publication.

Data must be archived such that:

- In such a way that an academic staff member from the same discipline can understand and verify that data, and possibly recreate the research;
- it is accessible in the long term, i.e. stored in a future-proof format (see appendix 4.1).

Non-digital data must be duplicated in digital or non-digital form, so that both the researcher and the Faculty can keep a copy. If it is not possible to make a duplicate, then the data must be stored at the Faculty whereby the researcher will have unrestricted access, including after they leave the employment of the University.

11. FAIR data

University of Groningen policy is to have, in principle, all data FAIR. Below, the general requirements that the data (and software and scripts) must meet at the UG are integrated into the presently accepted terminology of the FAIR principles. The data are:

Findable:

- Data is sustainably stored and curated;
- Data is provided with metadata, including affiliation and, if possible, with a persistent identifier;
- Data is registered on the basis of metadata in the research database of the university.

Accessible:

- Data is accurate, complete, reliable, authentic and provided with metadata and, if possible, with a persistent identifier;
- Data is available for checking and further research after completion of the research and/or the departure of the researcher;
- Data is openly available, unless valid reasons prevent this.

Interoperable:

- Data is stored in sustainable file formats;
- The discipline specific standards for the enrichment of data are applied;
- Data (and metadata) is provided with references to other relevant material.

Reusable:

- The origin of the data and the affiliation of the researcher involved is clear (Provenance);
- The discipline specific standards for data management are applied;
- The conditions for reuse are clearly described.

There may be sound reasons not to make data FAIR, however. To reiterate, this policy is based on a “comply or explain” principle, meaning that exceptions to this policy are possible. A researcher may wish not to make the data publicly available when:

1. Making the data publicly available would contradict any agreement or undertaken given as part of the informed consent process;
2. Where public release might have negative consequences for the people researched;
3. When there is an obligation or objective to protect results so that they can commercially or industrially exploited (or reasonably expected to be exploited);
4. Where public release could represent a security concern;
5. If open access would jeopardize achievement of the main aim of the research;
6. If there is any other legitimate reason not to publish the data.

If any of these reasons is to be claimed, the researcher can indicate this in the data management plan.

12. Data retention period

Data gathered for scientific, historical or statistic purposes should be stored for a period of at least ten years (to enable scrutiny in relation to concerns about matters of scientific integrity).

Data can be kept after a period of ten years for historical, statistical or research purposes, provided that the researcher has applied appropriate technical and organizational measures to protect the data, such as anonymization or pseudonymization (see section 10).

13. Reuse of data

Research data can only be reused under a couple of conditions:

- The researchers will anonymize the data where this is possible. Anonymized data is in principle available to research participants and anyone that requires it for research purposes or issues of integrity.
- Data that cannot be anonymized will not be available for reuse and can only be requested when integrity issues are at stake.
- Reuse should be on a request basis. The researchers should assess and decide if the data can be reused. This way, the researcher or institute can decide on a case-to-case basis whether the request aligns with the agreements established in the consent form participants have signed.
- In case a request involves something that has not been established in the consent form, the researcher will discuss this specific possibility for reuse with the research participants.
- The possibility of reuse should be indicated on the data management plan or be registered in the form of the Research Ethics Committee.

14. Responsibilities

Responsible data management requires collaboration between research and support services. There is joint responsibility for research data management within the UG. The guiding principle here is the Higher Education and Research Act and the elaboration thereof in the Administration and Management Regulations UG which allocates the responsibility at different levels. Within the faculty, the responsibilities are distributed:

14.1 Researchers

The researcher is responsible for drawing and implementing a data management plan (or having it implemented) for all her or his ongoing research during which research data is processed. The following is requested from the researcher:

1. To act in accordance with the General Data Protection Regulation, the General Policy for the protection of personal data of the UG and other statutory and ethical rules;
2. To record the arrangements made regarding data management during a (joint) research project or research contract in accordance with the Research Data Policy of the institute and the Netherlands Code of Conduct for Research Integrity. Appendix 2 indicates in which cases the researcher must record agreements in writing and which points have the attention of the General Administrative and Legal Affairs Service (ABJZ);
3. To safeguard the integrity and security of the data in accordance with the security baseline developed by the CIT;

4. To submit proposals for the destruction of research data, in advance, to the Research Director and/or the research ethics committee;
5. To assure the access, reuse and storing of research data after the end of the research project, in accordance with the research institute's data management plan;
6. To assure the storing and access to data management plans and data management protocols (incl. agreements with research partners);
7. To estimate the costs of – and investment of time in – data management during the research project and thereafter;
8. To familiarise oneself with new developments in the field of data management in the relevant discipline;
9. The co-development and documentation of the procedures and processes (suitable for the research) used for the collection, storage, processing, use and access of the research data;
10. To provide students and young researchers with guidance concerning good data management.

14.2 Graduate Schools

The Graduate Schools will embed the topic of data management in the early stages of researcher's careers, as an integrated part of scientific practice.

1. The Graduate Schools will provide mandatory courses for Research Master's students and PhD students and can make use of central services to this end;
2. The Graduate Schools will ensure that arrangements are made with PhD students regarding data management and the recording of such arrangements in these students' training and supervision plans.
3. The Graduate Schools will ensure that PhD thesis supervisors and the daily supervisors of the PhD students make arrangements, together with the PhD student, for the PhD student's research data to be made available for further research after the PhD programme has concluded (Regulations of the conferral of a doctorate (PhD regulations) Art. 4.1.5.).
4. The Graduate Schools will ensure – with support from the GDCC – that best practices in the field of data management education are shared.

14.3 Faculty Board and Centre for Religious Studies

The faculty board has a care duty to the researchers, and (PhD) students. They are responsible for setting up, maintaining and overseeing the implementation of a responsible data management policy in accordance with the UG Research Data Policy. The following responsibilities can be discerned:

1. The Faculty Board will provide and maintain an Institute's Research Data Management plan in accordance with the principles formulated in the Science Europe guidance and will make this data management plan available to its researchers.
2. The Faculty Board will adopt the Institute's Research Data Management Plans, after testing these against the stipulated frameworks. The plans will be published on the website of the Digital Competence Centre;
3. In the event of an externally funded research project, the institute will verify, in a timely manner, whether that research project's data management plan is in keeping with the research institute's data management plan.
4. The Faculty Board will maintain oversight and will supervise the enforcement of the rules related to data storage and management;
5. The Faculty Board will be responsible for ensuring that the data files, data management plans and research protocols can be verified, on the instructions of the Board of the University, if there is cause to do so (in the event of an alleged breach of integrity, for example);

6. Decision-making regarding the destruction of research data will be in the hands of the Center for Religious Studies, based on the protocols and/or the data management plan, where necessary in consultation with the Research Ethics Committee;
7. Both will cooperate with the periodical internal audits carried out to verify actual and ongoing compliance with the relevant rules and procedures;
8. The Faculty Board will, in consultation with the Centre for Religious Studies, determine which preconditions apply to the research data management during research in which third parties have control (or joint control) over the data;
9. The Faculty Board will make further arrangements regarding oversight over the research data after completion of the research, and regarding oversight over research data ensuing from the research by researchers who have left the University of Groningen;
10. The Faculty Board will ensure that data management, in conjunction with a focus on research integrity and on dealing with personal data responsibly, is enshrined in the curriculum;
11. The Faculty Board will draw up a policy and procedures for research data that is generated and used in the context of teaching. These guidelines are expressed in the Teaching and Examination Regulation Models. The learning outcomes expressly stipulate that, during research assignments, students must adhere to the applicable (discipline-specific) standards, not only at the publication stage, but throughout the entire research process. This, therefore, also concerns standards related to ethics, research integrity when dealing with data, and data management. ABJZ provides an optional additional provision in the Teaching and Examination Regulation Models;
12. The Faculty Board acknowledges the contribution made by ethics boards, in terms of advice regarding responsible data management and open data; it also encourages the exchange of knowledge between ethics boards;
13. The Faculty Board and research director encourage the exchange of knowledge and good practices among researchers;
14. The Faculty Board decides, in consultation with its research institutes and its Graduate School, by mutual agreement, which central data management services it wishes to use, and which aspects it will provide itself.

14.4 Research Ethics Committee

The faculty's Research Ethics Committee is an important actor within the faculty when it comes to responsible research data management. The REC has the following specific responsibilities:

1. The Research Ethics Committee is tasked with providing approval of research of researchers and PhD candidates appointed at the Faculty of Theology and Religious Studies of the University of Groningen.
2. The approval is limited to the quality of reflection and measures taken by the faculty member on matters of research ethics, data protection and data management of the research.
3. The ethics committee provides solicited and unsolicited advice to the Faculty Board and to staff members relating to measures on research ethics, data protection and data management of research by staff and by students.
4. The ethics committee regularly reviews forms and procedures on matters of research ethics, data protection and data management of the Faculty, to ensure new insights with regard to these topics are included. Such insights can come from experience within the Faculty or the University, but also from national and international developments.
5. The ethics committee is available to provide policy advice on education on research ethics.
6. The ethics committee provides a yearly report on its activities to the Faculty Board.

15. Data ownership

A specific case in which responsibilities may shift concerns the question of ownership of data. In principle, the data is jointly owned by the researcher and the institute (Faculty). In the case of personal data, the data belong to the research participant.

Unless there is a specific agreement to the contrary, responsibility for data *management* relating to the data from a specific research project will be regarded as the responsibility of the principal investigator or PhD researcher indicated in the RDMP submitted for that project.

Responsibility for data in cases when the researcher leaves the University
If a researcher leaves the employment of the institute, they retain their right of use. All data that must be retained will remain at the institute; the researcher is permitted to keep copies. All agreements on confidential data in the data management plan remain intact. It will be expected that all data (anonymised) will be deposited in the Faculty Research Data Repository in an appropriate form. For ongoing projects that are to remain at the University of Groningen, an alternative principle investigator is to be nominated. Where a project is to be transferred to the new institution, this will need to be recorded in the RDM system.

Responsibility for data when a researcher joins the University transferring a project
In the case of a finished project, it will normally be expected that the previous institution will manage the data storage provisions into the future. In cases where a staff member transfers a project, the Faculty will accept responsibility for the project and future data storage responsibility.

Ownership and responsibility of data when cooperating with other organizations/institutions
This will be decided on a case by case basis, but for each project there must be a clear determination about which institution will be responsible for management of data and compliance with the requirements of the European General Data Protection Regulation. The institutions will stipulate their responsibilities in either a data processing agreement or a joint controller agreement. General Administrative and Legal Affairs Service (ABJZ) can provide a template and further legal support.

Responsibility for enabling the exercise the rights of participants under the GDPR
Personal data ultimately belongs to the research participants who gave their data. Under the GDPR, research participants have a right to inspect or rectify their data. They may also submit a request for data erasure (‘the right to be forgotten’), restriction of the use of their data or they may object to data processing (art.15-18, 21 GDPR).

The general stance of the faculty is that the research team should try to accommodate these requests where they can, unless this is practically disproportionate in terms of time and effort, or if meeting the requests is likely to render impossible or seriously impair the purposes of the data processing. The GDPR offers several derogations for research purposes. In a case in which a researcher wants to claim one of these derogations, it is expected that legal support is sought.

In case of research is carried out in a team, the PI is primarily responsible for handling the requests of participants and handling further communication.

16. Data management and student research

The main focus of this data management plan is on research activities performed by (temporary) staff and PhD students. Students may also work with personal data and they may publish their findings as well.

The faculty cannot assume responsibility for student research activities if these are unsupervised, and undertaken as extracurricular activities. or if these take place as part of an internship at an external company or institution and there is no further involvement of lecturers/researchers.

Student research activities do fall under the responsibility of the UG if the research activities are part of the educational programme for which the student is enrolled (e.g. part of a course, if EC's are granted, or when the activity is compulsory). When the research activities take place as part of an internship at an external company or institution, then good datamanagement is a joint responsibility of the Faculty and the external party.

In terms of data management/GDPR/ethics, actions have to be taken in case:

- results of research are published, not only in journals but also for example in conference papers
- If students are collecting primary data (personal data) themselves.
- If students share data with an external party, or when they obtain access to data provided by the external company.

These actions are:

- Students will need to produce a data management plan as part of the preparation for the Bachelor's or Master's Thesis;
- Students and/or their supervisor should register the project in a suitable tool (RDMP-webtool, or the Research Gateway);
- in case of personal data a check whether further steps are necessary (e.g. signing data processing agreements, technical and organizational measures or even a DPIA).
- Students need to create a data package for their theses.

What the faculty/UG need to provide are:

- A clear data management instruction manual, in line with this data management policy. These instructions will not cover all aspects of data management to the same extent, but should include at least: the GDPR, informed consent, how to make a data management plan, use of data collection tools (e.g. Qualtrics), storage, sharing and archiving instructions of the data package, security.
- A clear format or tool for making a data management plan, with a distinction between Bachelor and Master students and a distinction between personal/non-personal scenario's.
- Proper IT facilities for collecting, storage and archiving data suitable for student use.
- Training in data management, and guidance by lecturers (see 'Training').

17. **Monitoring compliance**

The Faculty Board will maintain oversight and will supervise the enforcement of the rules related to data storage and management.

All research data management plans should be stored on the Y drive in the project folder. The secretary of the CRS will periodically check whether a data management for each project is available. When researchers do not submit a RDMP within the 3 months of commencement of the project, they will be sent a reminder to do this as soon as possible. If there is no RDMP sent after this period, then the Faculty Board will be informed.

At the time of the 9 month go/no-go interview, all PhD candidates will need to declare that they are familiar with the Dutch Code of Conduct for Academic Practice; that they will obey this code. They will also be required to have completed a Research Data Management Plan.

On completion of their PhD studies, the promotor will be responsible for ensuring that the PhD student will lodge all research data in the repository. When the data is stored, the promotor can indicate this in Hora Finita.

The policy of the University of Groningen is that PhD students can only defend their thesis when there is a data package for each empirical chapter of their dissertation. This implies that the graduate school will not send out the thesis to the reading committee before the packages are in place.

Lecturers are responsible for assessing the data management plans that students produce for their bachelor's or master's theses. The DMP's should be a necessary item on the assessment forms. Without a dmp, the supervision agreement cannot be signed and supervision cannot take place. The faculty will produce a separate plan that describes the requirements for students.

18. **Training**

Training of staff members and students is one of the priorities of the Privacy and Security plan of action for 2021-22.

Data management must be made an integral part of teaching and instruction, for example in the course unit 'Methods and techniques of research', during thesis seminars and methodology clinics and as part of the instruction on academic integrity during the Bachelor's and Master's degree programmes. Students should make a data management plan as a part of the preparation for the bachelor's and master's theses.

Implementing the training of students in data management in the curriculum is the responsibility of the Programme Director. A separate plan including a manual for data management will be drawn up.

PhD candidates can ask the Digital Competence Centre to help them draw up their data management plans (dcc@rug.nl). The DCC also offers e-learning modules on academic integrity and data management for staff members, PhD candidates and students.

19. **Costs of data management**

Taking appropriate technical and organizational measures might involve making extra costs.[15] Researchers should take this into account when they determine a suitable budget for their research project. This should encompass the costs of data management throughout the entire lifecycle and any additional costs for the necessary protective measures if sensitive research data are to be processed.

The Funding Officer and the Project Controller can help researchers preparing a budget.

The Board of the University and the faculties fund the general facilities for the purpose of research data management. For specific facilities, the costs are charged to the faculty. The funding of data management costs, including archiving, are included in each initial research proposal chargeable to the research funder.

[15] E.g. for the use of special IT-solutions.

The digitization of non-digital data can be included in the budget for a grant application. In other cases, researchers can discuss the options with their supervisor and the Managing Director of the Faculty.

20. Support

There are several possibilities for support at each stage of your research project:

- Digital Competence Centre:
  The DCC is the one-stop for research IT and data management. They provide advice, training, or IT support for researchers on all data management related matters. The team consists of employees of the University Library and the Centre for Information Technology, who cooperate closely with research support experts within their own institutions and the faculties. The Digital Competence Centre has data protection specialists who researchers can approach with questions about storing, archiving and reusing confidential and other data.

  Contact: dcc@rug.nl
  Web: https://www.rug.nl/digital-competence-centre

- Ethics Committee:
  The Ethics Committee provides solicited and unsolicited advice to the Faculty Board and to staff members on matters of research ethics, privacy and data management of research by staff and students. The Ethics Committee provides formal approval of research projects of researchers and PhD candidates appointed at the Faculty of Theology and Religious Studies of the University of Groningen when such formal approval is required.

  Contact: ethicscommittee.ggw@rug.nl
  Web: https://www.rug.nl/research/centre-for-religious-studies/research-ethics-committee?lang=en

- Privacy and Security Coordinator:
  A P&S coordinator gives advice on and information about all matters relating to data protection, and he/she performs checks on data protection compliance. A P&S coordinator is the first point of contact in the faculty when it comes to questions about privacy, taking appropriate measures, or starting with a DPIA. The P&S coordinator is also an advisory member to the Ethics Committee.
  Contact: h.a.ten.have@rug.nl
  Web: www.rug.nl/mu/privacy

- Demand Manager:
  Demand Managers are the link between the faculties and service units and CIT. They draw up inventories of the IT requirements of the faculties and service units and submit them to CIT as either desirable or necessary. A Demand Manager is also the person to contact about IT hardware or software requirements. Suitable solutions will be sought together.

  Contact: demandmanagementict@rug.nl
  Web:
  https://myuniversity.rug.nl/infonet/medewerkers/ict/beleidenprojecten/demandmanagement/

21. Actions required of the Faculty

- The Faculty needs to help develop and implement the Research Gateway Tool produced by the Faculty of Behavioural Sciences.
- The Faculty needs to develop a plan for managing data processing activities of students, produce a separate instruction for data management.
- The Faculty and the DCC also need to develop IT facilities for students for proper data management, such as storage facilities.
- The Graduate School needs to monitor PhD students to ensure that they comply with the research data requirements.
- The Graduate Schools will ensure – with support from the DCC – that best practices in the field of data management education are shared.
- The Research Ethics Committee will participate in the UG network of Ethics Committees to exchange knowledge and best practices.

22. Concluding remarks

Research data management is a relatively new field of expertise. During the coming years, the existing policies will need to be reviewed regularly and changed where necessary. At the same time, new and better infrastructures and resources to support data management will become available. This policy memorandum will therefore also have to be regularly reviewed and updated.

Appendices

Appendix 1: Preferred Data Formats[16]

Data type	Preferred format	Acceptable format
Documents	PDF/A (.pdf) Unicode TXT (.txt)	OpenDocument Text (.odt) MS Word (.doc, .docx) Rich Text File (.rtf) PDF (.pdf) Non-unicode TXT (.txt)
Spreadsheets	PDF/A (.pdf) Comma separated values (.csv)	OpenDocument Spreadsheet (.ods) MS Excel (.xls,.xlsx)
Databases	ANSI SQL (.sql) Comma separated values (.csv)	MS Access (.mdb, .accdb) dBase III or IV (.dbf)
Statistical data	R	SPSS Portable (.por) SAS transport (.sas)
Video	MPEG-2 (.mpg, .mpeg, …) MPEG-4 H264 (.mp4) Lossless AVI (.avi)	QuickTime (.mov)
Pictures (vector)	PDF/A (.pdf) Scalable Vector Graphics (.svg)	Adobe Illustrator (.ai) PostScript (.eps) PDF (.pdf)
Pictures (raster)	JPEG (.jpg, .jpeg) TIFF (.tif, .tiff)	
Audio	WAVE (.wav)	MP3 AAC (.mp3)

[16] http://www.rug.nl/research/institute-evolutionary-life-sciences/data-management/repository/procedure_gelifes_data_repository_v3.pdf

Appendix 2: Overview of available storage solutions (2022)

Depending on the type of project, the following table helps you find the most suitable storage solution *during* your research project:

For my project, I will be… **… and can I use…**	… storing personal data	… storing special personal data/more sensitive data	… storing other valuable data but no personal data
… the X Drive UG account (X:\)	Yes	Yes	Yes
Y Drive UG account (Y:\student\ggw)	Yes	Yes	Yes
Google Drive UG account	Yes	No	Yes, recommended for collaborating on shared files.
Google Drive personal account	No	No	No
Unishare (UG managed)	Yes	Yes, this drive also features extra privacy controls.	Yes
Dropbox, OneDrive, iCloud or other third-party cloud storage solution	No	No	No
Personal laptop, or other personal device	Recommended *during* research if the security of the device is up to date, *and* there are no online possibilities for storage available (e.g. on a remote location) *and* when encryption is applied.	Recommended *during* research if the security of the device is up to date, *and* there are no online possibilities for storage available (e.g. on a remote location) *and* when encryption is applied.	Yes, but also keep the security of the device up to date and please do make regular backups.
External harddisk, USB drives	Recommended if there are no online possibilities for storage available (e.g. on a remote location) and when encryption is applied.	Recommended only if there are no online possibilities for storage available (e.g. on a remote location) and when encryption is applied.	Recommended only if there are no online possibilities for storage available (e.g. on a remote location) and when encryption is applied.
Locked drawer/cabinet in locked room	Yes (e.g. consent forms)	Yes	Yes

NB: if you decide to encrypt data, then please keep in mind that if you forget the key, you will no longer have access to the data.

NB 2: Please also think about making backups! The X/Y drives also have a backup function. The CIT department can restore the data up to 90 days after the incident.