university of groningen / faculty of spatial sciences / ursi

Research Data Management Policy and Procedures

Faculty of Spatial Sciences (URSI)

Final version, 2 March 2023

Table of Contents

1. Introduction

The social standing of academic inquiry and of universities in general will only be maintained and enhanced if all research is done in an appropriate and ethical manner, including protecting the confidentiality of personal information, while at the same time enabling peer review and verification of data.
To protect people during research, especially vulnerable people, means supporting good practices that deal with data management and ethical aspects.

This document outlines the general policy relating to Research Data Management (RDM) in the Faculty of Spatial Sciences, and it lays out what is expected of staff and PhD students based in the Faculty. The document links to and needs to be read alongside other documents such as the policies on research ethics. For the learning environment of bachelor and master students a 'light' version of this data management policy is applicable, while learning skills on data management is part of the educational programme.

This document is updated regularly and aligned with the central RUG research portal (https://www.rug.nl/research/research-support-portal/) and follows a range of procedures and protocols that have been implemented at European, Dutch and University levels. Of particular note is the legal requirement of the university to comply with the European General Data Protection Regulation (GDPR). It is therefore important that staff and PhD researchers are aware of and comply with this policy and the requirements and general expectations it discusses.

The Faculty's overall position is one that accepts that its academic staff and PhDs are professional and competent, but acknowledges that it is the Faculty's legal and social responsibility to provide appropriate oversight and monitoring in an efficient way.

2. Governance and standing of this document

This revised research data management (RDM) policy document was developed in response to the UG Research Data Policy 2021, and is consistent with university trends around the world. 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 Faculty's URSI Research Data Repository: Storage Protocol

Furthermore, the following documents provide extra context:

- the 2017 University of Groningen Code of Conduct on Integrity
- the 2018 Netherlands Code of Conduct for Research Integrity
- the European Code of Conduct for Research Integrity
- the European General Data Protection Regulation
- UG Research Data Policy 2021
- the 2018 Code of Ethics for Research in the Social and Behavioural Sciences involving Human Participants (Nethics)

3. Scope

The subject matter of this policy is the proper management of all data processed in research activities at the Faculty of Spatial Sciences and research data processed in collaboration with national and international research partners. Specifically relevant here are ‘Personal data’. Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it’s relatively easy to ID someone from it.

‘Data’ should also be taken as ‘digitized data’. Data that exist in paper format (e.g. questionnaires) fall within the scope of this plan only to the extent to which they can be digitized.

4. Rights and responsibilities relating to this policy

This policy document and the procedures in it apply to all staff involved in research and all PhD students in the Faculty. For students the Data Protection Guide for Student Research has been developed in the context of the learning environment, when writing a bachelor or master thesis or an article. This is described in section 11.

Researchers are regarded as being responsible in their own right for compliance with these requirements and are expected to follow the current procedure of ethics approval, overseen by their supervisors. Apart from familiarity with the expectations of research data management in general, for each specific research project or PhD project, the following requirements apply.

1. Shortly after commencement of a research project, the principal investigator (for a funded project to a staff member) or PhD student (for a PhD project) needs to complete a Research Data Management Plan using the online tool available (click on this link) in anticipation of other tools which might be implemented in the context of the RUG wide Research gateway. This must be done for all projects irrespective of their data requirements. In situations where there is no use of data, the RDMP Tool is very easily completed, but must be done to ensure that the Faculty is exercising its oversight responsibility. Should there be a significant change to data or methodology over the course of a project, it is the researcher’s obligation to provide an update to the RDM Plan and to revise what is stored on the RDMP Tool. Researchers will be expected to adhere to the plan (as updated from time to time) and that they and the Plan comply with the expectations described in this document.
2. Near completion of the research project, the principal investigator or PhD student will need to archive all data in an appropriate digital and anonymised form in the Faculty Research Data Repository. This is currently the Y-drive on the University’s network until a RUG wide repository has been installed. The researcher’s data should also be accessible by the supervisor, at least when the PhD project has ended.
3. Repositories such as Dataverse are also allowed, e.g. in case of EU-funded projects: https://www.rug.nl/digital-competence-centre/research-data/archive-and-publish/

5. Overarching principles

This policy is informed by several key overarching principles that govern research at the University of Groningen and at universities in general:

- All research is to be undertaken in an ethical and legally responsible manner, paying due respect to all participants in the research process, and in accordance with relevant legislation. Although there are many aspects to ethical research, the concept of informed consent is fundamental. Essentially, 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. With regard to research ethics policies and standard academic integrity we refer here to the RUG policy which is based on the Netherlands Code of Conduct for Research Integrity 2018. https://www.rug.nl/about-ug/policy-and-strategy/research-ethics/?lang=en
- Research also applies to student research, carried out in the context of a bachelor or master thesis or the writing of an article. Learning skills on data management is part of the educational programme. This is elaborated upon in section 11.
- 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. When possible, data needs to be anonymised.
- 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 of the integrity of the data.
- Where research is publicly funded, the results of the research should be made publicly accessible, either through the provision of open access publications or by making short summaries available.
- Where feasible and ethically appropriate, researchers will make their data FAIR (see section 12).

6. Research data management throughout the whole research process

(1) Planning research and data needs

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, especially the requirement to anonymise the data as soon as practical. 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. The resulting research data management plan should be registered via this link.

(2) Data collection

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. Ideally, data is stored directly onto the Y: drive.

During field work, data can be stored initially on a personal computer or laptop if there is no internet possibility. The data will need to be uploaded onto the Y-drive regularly (depending on the circumstances). It is recommended to also upload on an encrypted external hard-drive and then delete data from the laptop. It is also good practice to encrypt the partition of the harddrive reserved for storing personal data. In case of loss or stolen laptop/devices this needs to be reported as a data breach via cert@security.rug.nl.

(3) Access to data during the research process

Except for legitimate requests relating to scientific integrity concerns, it is generally advisable to restrict access to data to the researcher and supervisor(s) only, and restrict access until such time that the researcher is completely sure that original research data have been verified (for coding accuracy) and maybe until all publications being produced from the data are finalised. However, all research participants have a right to see any data that pertains directly to them, and can request that data which refer to the research participant will be removed from the data set where this is feasible.

(4) Storage of data

In line with the Netherlands Code of Conduct for Scientific Practice and the policies of the University of Groningen, empirical data is required to be stored safely. In anticipation of a RUG wide repository, the Faculty manages a Research Data Repository (Y-drive). The FSS repository is in a digital form where every researcher has their own folder identified with a P-number. Researchers will be required to provide their data in an appropriate form (including anonymization). The function of the Faculty repository is to enable access only under certain specific circumstances relating to the need to be able to verify the data. The URSI Director in consultation with the researcher will be responsible for assessing any request to access data in the repository. Consistent with the prevailing requirements, data will be stored in this repository for a fixed period of 10 years. After 10 years, data that has not been made open access will be destroyed, though if needed data can be stored longer. Note that all data must be fully anonymised as soon as practical to do so.

Note that the Faculty data repository is not an open access facility, it is merely established to allow scrutiny in relation to legitimate concerns about scientific integrity. To comply with the open access expectation, researchers might need to identify an appropriate open access data provider, such as might be provided by a scientific institute or a journal publisher.

(5) Cybersecurity

A cyber security incident is a situation involving a breach of the security of the UG's information systems and the data stored within them. A data breach is a situation in which the security of personal data has been compromised.

Examples of a cyber-security incidents and data breaches are:

- A laptop gets stolen or is lost.
- A data set containing personal information has been accidentally shared with a number of people who should not have access.
- A couple of signed consent forms have been left in public transport.

Always report cyber security incidents (whether these are confirmed or suspected) and data breaches to the Computer Emergency Response Team via cert@security.rug.nl. This contact desk is also available for reporting incidents that require confidentiality.

7. Responsibility for data management

‘Ownership’ is a word with legal implications, and strictly speaking the ownership status of data is complicated by the employment status of the researcher as well as of any grant funding received. Nevertheless, irrespective of the formal ownership of data, all researchers have a responsibility for care of data; and the University of Groningen has a responsibility relating to any research done under its auspices. Therefore, 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 team (PhD student and supervisors), indicated in the RDM Plan submitted for that project.

Responsibility for data in cases when the researcher leaves the University
In the case of a PhD researcher finishing their PhD or a staff member leaving to go to another institution, for all completed projects, it is expected that all (anonymised) data will be deposited in the Faculty Research Data Repository in an appropriate form, accessible by the researcher and supervisor(s). For ongoing projects that are to remain at the University of Groningen, an alternative principle investigator is to be nominated.

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.

8. Using personal data

In some cases researchers process personal data in their research. Researchers are therefore expected to understand the basic principles of the General Data Protection Regulation.

(1) The General Data Protection Regulation
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.

In case of secondary data, the researcher should check if consent is needed from the secondary data source. Also when using existing data, it is important that the respondent gave consent for these data to be re-used. (see https://www.nethics.nl/).

Examples of 'identifiers' are names, an identification number, contact details, location data, dates and times of meetings, 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 and requires us to properly secure the data.

We expect staff:

- to take notice of the general principles of the GDPR. A special UG website has been created to inform everyone in the UG about the basic principles;
- to take standard precautions when handling data. Among these are e.g. creating strong passwords, anonymisation when possible, working on secure devices and working on the university's network as much as possible. See the UG's website for a general overview of the standard measures that you can take;
- in case of handling personal data in research to be demonstrably compliant, by creating and registering a data management plan and applying for approval of the Research Ethics Committee and by checking whether a DPIA is necessary.

(2) Demonstrating compliance

A central principle in the GDPR is 'accountability'. If researchers are planning to process personal data in their research, then they need to be able to demonstrate compliance with the GDPR. 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.

Researchers are therefore expected to anonymise data when possible, design their research in a privacy-friendly way, think about appropriate technical and organizational measures, register their research proposal and follow the existing ethics approval procedure.

(3) Data Protection Impact Assessment (DPIA)

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[1] are likely to 'result in a high risk to the rights and freedoms of natural persons' (art. 35 GDPR).

An exhaustive list of potential high-risk scenario's cannot be given in advance, but in general, a DPIA may be necessary when researchers are planning to include sensitive personal data into their dataset (such as health data or ethnicity); when they involve innovative technologies (and companies) that process data; research with location data, GPS tracking of individuals or research that uses 'profiling techniques'; when people may be in a vulnerable position (children, or people who face imbalances in power relationships; or when they systematic monitor of publicly accessible areas without informing people ('covert observation'). Projects that involve many different partners with different (non-academic) aims may also be subjected to a DPIA.

—

[1] The European Data Protection Board has formulated a guidance document: 'Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)', (pp. 8 t/m 13). Retrieved on 2-2-2023 via https://ec.europa.eu/newsroom/article29/items/611236

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 performed by a team of people involved in the project in question, including, for example, a subject expert, a privacy officer, an IT expert, and a student or staff member involved. 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.

The Privacy and Security Coordinator can advise whether a DPIA is necessary. The decision to do a DPIA is ultimately the responsibility of the Faculty Board.

9. Role of the Graduate School in research data management

Some specific roles and responsibilities rest with the Graduate School. The Graduate School embeds the topic of data management in training activities for PhD researchers. Responsible data-management is an integrated part of scientific practice and is addressed in TSP plans and R&O conversations. GDPR is also part of the educational training for PhD candidates.

1. The RUG Graduate Schools provide mandatory training (e.g. on academic integrity) to Research Master's students and PhD students.
2. The Graduate Schools will oversee that PhD supervisors make arrangements with PhD students regarding data management and the recording of such arrangements in these students' Training and Supervision Plans (TSP). In the TSP PhD thesis supervisors make arrangements, together with the PhD student, regarding the PhD student's research data both during the project and (to be made available for further research) after the PhD project has concluded (Regulations of the conferral of a doctorate (PhD regulations) Art. 4.1.5.).
3. The Graduate Schools will oversee that PhD candidates complete an RDMP using the RDMP Tool.
4. The Graduate Schools will ensure – with support from the UG DCC – that best practices in the field of data management education are shared.

10. Education, data management and student research

The main focus of this data management plan is on research activities performed by (temporary) staff and PhD students. Training is offered by UG to staff and PhD candidates to develop skills in data management. Students may also work with personal data and they may publish their findings as well. Their research activities therefore fall under the responsibility of the Faculty if the research activities are part of compulsory course units under supervision of a staff member, i.e. a bachelor and master thesis or a publishable journal article. As data management is a learning process like others, making mistakes is part of this process. Teaching students how to learn and improve skills on data management is part of the educational programme (for example in the course Methods of Academic Research).

In terms of data management/GDPR/ethics, actions are restricted to the following educational activities, and only in case:

- students are collecting primary data (personal data) themselves for compulsory course units of the degree programmes for the Bachelor's and /or Master's thesis.
- the results of research are published, not only in journals but also for example in conference papers.

These actions are:

- Students make a data management plan as part of the Bachelor's or Master's Thesis process if it includes personal data (for example retrieved via interviews). This also includes a dedicated paragraph in the written thesis.
- The student should follow instructions to handle data in a correct way (checked by the supervisor), storing the data in a secure place, protected by two-factor authentication, adhering to good practice.
- The Faculty and the CIT are responsible for offering the student a secure storage space. This will be the Y-drive by default, unless the project requires otherwise (to be determined case by case).
- Students and/or their supervisor should register the project in a suitable format once the RUG Research Gateway is in place.

The thesis supervisor(s) are responsible for guidance concerning good data management. The Faculty Board is responsible for creating guidelines concerning data management of research performed by students.

11. Implementing open science, FAIR principles, and open access to data

One of the University's policy goals is to make, 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.

Furthermore, open science and FAIR principles need to be integrated in the data process as much as possible. 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 datamanagement plan.

12. Awareness-raising about data management

The Faculty will take appropriate steps to inform staff and PhD students about the policy and expected procedures. Specifically, from January 2018 on, all new PhD candidates will be required to complete training covering research ethics and research data management issues. Furthermore, a special section in the PhD Training & Supervision Plan shall be dedicated to data management. The Faculty will take care that procedures of dealing with data are properly embedded in the educational programmes.

Sharing Good Practices

The URSI Faculty Research Institute will emphasize sharing good practices amongst their researchers and PhD students. This will be done by means of:

1. Organizing URSI (lunch) seminars with RDM as a central theme, thereby inviting and encouraging URSI staff and PhD students to attend.
2. Inter-faculty platforms that stimulate the exchange of knowledge and best practices on RDM. These platforms are, amongst others, the privacy- and security officer meetings and the faculty funding officers meetings.
3. Attending national platforms for ethical committees.
4. Formulating requirements on data management for BSc and MSc theses, to make this part of students' learning paths.

Training

Awareness-raising about research data management is also realized by organizing workshops and training for our researchers and PhD students. These workshops have the aim to educate our researchers and PhD students in conducting responsible research.

For PhD students the workshop Academic Integrity is organized twice a year. RDM is a central theme during this workshop. Academic Integrity is a mandatory part of the URSI PhD program; the educational program for the PhD students of the Graduate School. Also, a RDM Workshop is being developed. This workshop is targeted at helping PhD students with the development of their RDM Plan in the Tool. Also, immediate feedback is given.

13. Ensuring compliance

The Faculty Board will maintain oversight and will supervise practices related to data storage and management.

Researchers are responsible for submitting an RDMP within 3 months of commencement of a research project. A CIT/Library Data Steward is available for advice and reminders.

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 using the Research Data Management Tool.

On completion of their PhD studies, the PhD team (PhD student and supervisors) will be responsible for ensuring that the PhD student will archive all research data in the repository. The data should be accessible by the supervisor after the PhD student has left. On termination of the contract of a staff member, data should be lodged in the repository.

14. Roles and Tasks

1. This document needs to be read and used alongside the following documents:
   - the Faculty's policy and procedures on Research Ethics
   - the Faculty's URSI Research Data Repository: Storage Protocol
2. Researchers are responsible for following the aforementioned protocols, submitting a research data management plan for each project in the RDMP web tool (https://rdmp.webhosting.rug.nl/) and for archiving their data in the Faculty Research Data Repository.
3. The Data Steward (CIT/Library) is responsible for providing feedback to researchers on their data management plans and the storage of data in the Faculty Research Data Repository.
4. The Privacy and Security Coordinator is responsible for assessing data protection risks of research projects, for coordinating the DPIA-process and for further supporting researchers in taking risk mitigating measures.
5. The URSI director is responsible for providing instructions on data storage, the RDMP webtool and DMP formats, in collaboration with the Data Steward (CIT/Library) and for communicating data management policy to researchers, students and PhD students.
6. The Faculty's director of Education, in collaboration with the Privacy and Security coordinator, is responsible for making a plan for training students in good data management practices and for embedding data management in the curriculum.
7. The CIT is responsible for providing suitable IT facilities for collecting, storage and archiving data for staff and students, on request of the FB.
8. The Departmental chairs are responsible for investigating the needs of staff members for further training in data management skills.
9. The Data Steward aligns data management procedures with other Faculties within the University.
10. The Data Steward supports the Faculty in implementing the Research Data Management System.

Applicable definitions

FAIR-data stands for findable, accessible, interoperable and reusable data. This means that data or datasets should be archived in such a way that ideally the research results can be replicated. Metadata and data should be machine-readable in order to make it easy to find; anyone who finds the data should be able to know how they can be accessed; the data needs to interoperate with applications or workflows for analysis, storage and processing and, when there no objections the metadata and data should be well-described so that they can be replicated and/or combined in different settings.

Data Steward is an officer (at CIT/Library) who is responsible for managing and protecting an organization's data. They are responsible for making sure that data is stored, used, and shared in a way that is secure, compliant with relevant regulations, and aligned with the organization's goals and policies. Data Stewards can support researchers in managing their data according to policy.

GDPR refers to Regulation 2016/679 of the European Parliament and of the Council: the General Data Protection Regulation. This legislation lays down the rules regarding the processing of personal data and it protects the fundamental rights and freedoms of natural persons when it comes to personal data.

Ius Promovendi is the legal right of an academic staff member (historically a professor) to award a PhD.

Personal data. The European Regulations defines 'personal data' as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

PhD research project means a research trajectory undertaken by a PhD student under the supervision of a Primary Supervisor.

PhD student means anyone enrolled in a PhD programme at the Faculty, irrespective of their status (part time/fulltime; internal/external, etc) or type of funding.

Primary Supervisor means the staff member who has primary management responsibility for the supervision of a PhD student (this might be the professor promotor, but it could also be an Associate or Assistant Professor).

Principal Investigator means the person who has primary responsibility for a research project. Every designated research project shall have a defined Principal Investigator.

Promotor is a person with an *Ius Promovendi* who is recorded as being the person who will eventually award the PhD to the PhD student and at least has nominal oversight of the PhD research (also see Primary Supervisor).

Research is a systematic process of investigation into a particular topic.

Research data means any data collected in the course of research for a specific research project.

Research Data Management refers to the concept about how research data should be managed.

Research Data Management Plan refers to the plan for how research data will be managed that is uploaded onto the Research Data Management Tool.

Research Data Management Policy refers to this document, the policy statement of the Faculty of Spatial Sciences on research data management.

Research Data Management Tool refers to the online management system developed and implemented in the Faculty.

Research Data Repository means the digital archive where research data will be stored by the Faculty for 10 years.

Research Project means a designated research trajectory, which could be a PhD research project or a research project undertaken by a staff member. A research project is normally identified by any of the following: any research activity the entails the collection of primary data or the extensive use of secondary data; the allocation of funding to conduct a specific research task; the appointment of research staff to undertake the research; a PhD trajectory; or any research activity that requires gaining research ethics approval. For each research project, a separate Research Data Management Plan must be submitted.

Researcher means anyone involved in a research project, including staff members and PhD students.

Staff means anyone employed by the University of Groningen in any capacity other than for the purposes of doing a PhD.

Comments on this Policy

Please direct comments on this policy to the Director of the Urban & Regional Studies Institute.

The Faculty Board of Spatial Sciences approved this revised policy document on 7 March 2023.