ArcticNet

ᐅᑭᐅᖅᑕᖅᑐᒥᒃ ᑐᑭᓯᓂᐊᖅᑎᑦᑕ

Data Management Policy

Contents:

Final Draft: 31 March 2021; Revised: February 2025

1. Introduction

ArcticNet is a Canadian research network that brings together scientists and managers in the natural, human health and social sciences with their partners in Inuit organizations, northern communities, federal and provincial government agencies, and the private sector to study the impacts of environmental change in the Arctic regions in Canada. The central objective of ArcticNet is to contribute to the development and dissemination of knowledge needed to formulate adaptation strategies and national policies to help Canadians face the impacts and opportunities of the transformation of the Arctic.

The wealth of knowledge and data generated by ArcticNet-funded research must be managed, to ensure and maximize the exchange and accessibility of relevant data, and to leave a lasting legacy. It must also recognize and support the goal of advancing Inuit, First Nation, and Metis access, ownership, and control over data and information gathered on their populations, wildlife, and environments.

The ArcticNet Data Management Committee (ADMC) was formed by the Research Management Committee (RMC) on 1 March 2006, and was tasked with developing the ArcticNet Data Management Plan that included the ArcticNet Data Policy (ADP), first published 18 January 2008 and updated 10 January 2011. ArcticNet commissioned a fulsome update of the ADP in November 2020, resulting in the ArcticNet Data Management Policy (ADMP) presented here.

The function of this document is to provide guidance on the objectives, principles, and guidelines for the management, retention, use, and dissemination of data generated and collected by ArcticNet-funded projects. The ADMP was created based on current best practices in research data management and in consultation with the *Tri-Agency Statement of Principles on Digital Data Management*[1] and *Research Data Management Policy*.[2]

2. Objectives

The central goal of the ADMP is to facilitate exchange of information about the Arctic regions in Canada among researchers and other user groups, including those in Inuit Nunangat, northern communities, and international programs. The specific objectives are to:

- implement data management best practices that include the highest professional and domain standards, nationally and internationally, to support research excellence in ArcticNet-funded projects;
- maximize the value of data collected and generated through ArcticNet-funded research by making results as accessible as possible to advance knowledge, avoid duplication, and encourage reuse, for the benefit of society, particularly for Inuit, First Nation, and Metis communities who are most impacted by it, and research communities;

[1] Government of Canada. (2015). *Tri-Agency Statement of Principles on Digital Data Management*. http://www.science.gc.ca/eic/site/063.nsf/eng/h_83F7624E.html.
[2] Government of Canada (2021). *Tri-Agency Research Data Management Policy*. http://www.science.gc.ca/eic/site/063.nsf/eng/h_97610.html.

- enhance the quality and impact of ArcticNet-funded research through encouraging increased FAIRness of data - that is, data which is Findable, Accessible, Interoperable and Reusable3;
- encourage scientific and interdisciplinary collaboration among ArcticNet-funded researchers, and the general research community, through clear mechanisms and mandates for responsible data sharing and recognition of the data providers;
- encourage responsible data sharing by providing guidance to ArcticNet researchers working with sensitive data; and
- recognize and actively support First Nations, Inuit, and Métis Nation data sovereignty and governance through adherence to community-generated research requirements, practices, and principles, such as the pan-Indigenous CARE Principles4 that ensure that Collective Benefit, Authority to Control, Responsibility, and Ethics are thoroughly considered in research involving Inuit, First Nation, and Metis peoples, lands, governments, communities, or organizations (further community- and region-specific, distinctions-based guidance, such as First Nations Information Governance Centre Principles of OCAP®5 and the Inuit Tapiriit Kanatami (ITK) National Inuit Strategy on Research6, are detailed in Section 10.2 Indigenous Research).

3. Principles

The overall principle guiding the ADMP is a view of publicly-funded research data as a public good that should be as open as possible to facilitate reuse, while also respecting privacy, security, ethical considerations and appropriate intellectual property protection. The following sub-principles further guide the responsible, effective and ethical management of data generated through ArcticNet-funded research:

- ensure ArcticNet data and metadata are made publicly available as quickly as possible, though restrictions may be placed on access where necessary to allow researchers to benefit from their efforts and to respect confidentiality, privacy and sensitivity requirements, Intellectual Property rights, compliance with government and community protocols and requirements, and researcher rights to publication;
- strengthen and advance the goal of ensuring Inuit, First Nation, and Metis access, ownership and control of data that is gathered on their population, wildlife, and environment;
- ensure ArcticNet data are citable, publishable, and acknowledged as valuable contributions to knowledge dissemination;
- ensure the preservation of data generated through ArcticNet-funded research (when appropriate);
- ensure that there are strong linkages to Canadian and international Arctic data management processes;

[3] Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. (2016). *The FAIR Guiding Principles for Scientific Data Management and Stewardship*. *Scientific Data, 3*(160018). https://doi.org/10.1038/sdata.2016.18.
[4] Global Indigenous Data Alliance (GIDA). (2019). *CARE Principles for Indigenous Data Governance*. https://www.gida-global.org/care.
[5] First Nations Information Governance Centre (FNIGC). (2020). *The First Nations Principles of OCAP®.* https://fnigc.ca/ocap-training/.
[6] Inuit Tapiriit Kanatami (ITK). (2018). *National Inuit Strategy on Research (NISR)*. https://www.itk.ca/wp-content/uploads/2020/10/ITK-National-Inuit-Strategy-on-Research.pdf.

- leverage existing systems and infrastructure, wherever appropriate (i.e., ensure connectivity and interoperability of data, while avoiding unnecessary duplication of systems) and observe and address any gaps or areas of needs; and
- support researchers in their efforts to establish and implement best practices for data management that are consistent with ethical, legal, cultural, and commercial obligations, as well as other funder requirements, through outreach, training, resources, and guidance.

4. Application

The ADMP applies to all data that is derived from research that is funded entirely or in part by ArcticNet. In situations where research is co-funded and data management policies differ between funders, ArcticNet reserves the right to consider how the ADMP is applied. This document will be reviewed periodically by ArcticNet and its stakeholders to ensure the principles and guidelines herein remain relevant. ArcticNet retains authority to revise this document as deemed necessary. In the event of revisions, consultations will be made with affected stakeholders.

5. Definitions

ArcticNet Data (hereafter, "data") are any and all data that have been collected and/or generated by ArcticNet researchers and collaborators in the performance of research initiatives funded by ArcticNet.

Data may take many forms, and depending on discipline and culture, can mean different things. This includes but is not limited to: survey results, written observations, software, interview transcripts, photographs, automatic measurements, hand-drawn maps, stories, video footage, audio recordings, and physical samples. Thus, the ADMP defines data as incorporating all ways of knowing: Western/academic, Indigenous, and local ways of knowing.[7]

ArcticNet Metadata (hereafter, "metadata") is the documentation providing information about the data, specifically the *what, where, when, by whom* it was collected, its current location, and any access information.

ArcticNet Researchers (hereafter, "researchers") are all Network Investigators (NIs) and highly qualified personnel (HQP; including students, research assistants [RAs], Indigenous researchers and knowledge holders, technicians, and postdocs) working on projects funded in whole or in part by ArcticNet.

Indigenous Knowledge reflects the unique cultures, languages, values, histories, governance and legal systems of Indigenous Peoples. It is place-based, cumulative and dynamic. Indigenous Knowledge systems involve living well with, and being in relationship with, the natural world. Indigenous Knowledge systems build upon the experiences of earlier generations, inform the practice of current generations, and evolve in the context of contemporary society. Different First Nations, Inuit and Métis communities each

[7] Government of Canada. (2017). *Data Management Principles and Guidelines for Polar Research and Monitoring in Canada*. https://www.canada.ca/en/polar-knowledge/publications/data- management- principles-and-guidelines-2017-may.html.

have distinct ways of describing their knowledge. Knowledge Holders are the only people who can truly define Indigenous Knowledge for their communities.

This knowledge is integral to a cultural complex that also encompasses language, systems of classification, resource use practices, social interactions, ritual and spirituality. These unique ways of knowing are important facets of the world's cultural diversity, and provide a foundation for locally-appropriate sustainable development.[8]

6. Data Management Plans

In accordance with international best practices and requirements from the Tri-Agency federal funding bodies, ArcticNet requires all projects to complete and maintain a data management plan (DMP) that describes how the data will be managed throughout the lifecycle of the project, including collection, documentation and metadata, storage and backup, long-term preservation, sharing and reuse, responsibilities and resources, and ethics and legal compliance. DMPs assist researchers in determining the costs, benefits and challenges of managing data, and should be consulted and updated throughout the research project. Often the details included in a DMP may be reused for writing research proposals, funding applications, abstracts, metadata, and other related reporting throughout a project.

The content and length of DMPs will depend on the nature of the project, but generally they describe the following (adopted from the *Digital Research Alliance of Canada DMP* [9]:

- **data collection** - how will data be collected and formatted;
- **data documentation and metadata** – how will data be documented and captured consistently;
- **storage, backup, and protection –** what are the data storage requirements and how will it be protected;
- **preservation** – where will data be preserved over the long-term and how will ongoing access to it be provided;
- **sharing and reuse** - how and when will data be shared and reused;
- **responsibilities and resources** - who will be responsible for managing the project's data during and after the project; and
- **ethics and legal compliance** – how will sensitive data be managed and what are the ethical, legal, and intellectual property constraints to which the data are subject.

These aspects are discussed in the following sections of this policy, and Appendix A provides further guidelines for writing a DMP. Researchers may also consider the use of a standardized tool, such as the *Digital Research Alliance of Canada's DMP Assistant*[10] to assist in developing DMPs.

[8] United Nations Educational, Scientific and Cultural Organization (UNESCO). (2017). *Local and Indigenous Knowledge Systems*. http://www.unesco.org/new/en/natural-sciences/priority-areas/links/ related-information/what-is-local-and-indigenous-knowledge
[9] https://dmp-pgd.ca/.
[10] https://dmp-pgd.ca/.

7. Data Quality and Metadata Standards

ArcticNet, in collaboration with the Canadian and international Arctic data management community, seeks to promote the highest standards in the stewardship of data and metadata resources resulting from its research activities. ArcticNet funds research across a variety of disciplines, including natural, human health, and social sciences, and as such, data covered by the ADMP are highly diverse in terms of data type, format, size, and management requirements. Researchers must therefore adhere to the data management best practices and generally accepted metadata standards used by their discipline or field.

Metadata standards are diverse and will vary across disciplines, but, when possible, common and generally accepted disciplinary standards are preferred (such as ISO 19115[11], FGDC[12], or Dublin Core[13]). Metadata should include, but not be limited to, records related to the collection, storage, and retrieval of data, as well as steps taken to process, analyse, and visualize data. At minimum, data must include clear supporting documentation and metadata sufficient for reuse and replication of results by other researchers.[14] Researchers may consult existing resources and guidance on achieving more detailed metadata and documentation, and additional support may be offered by repositories.[15]

Standardized metadata records consist of a defined set of fields that generally include, at minimum, who created the data and when, information on how the data were created, their quality, accuracy and precision, as well as other features necessary to enable understanding and reuse. Metadata records should be submitted to the data repository of choice as early as possible to indicate the presence of the data and project and may be updated regularly as the project progresses. Data that are described with rich metadata and documentation are inherently more findable, accessible, interoperable and reusable, and thus in alignment with the FAIR Guiding Principles.[16]

In their annual progress reports submitted to ArcticNet, URs are required, after the first year of receiving ArcticNet funds, to provide links to their metadata records that have been submitted to recognized data repositories or metadata storing facilities. Failure to submit openly accessible metadata records will lead to ArcticNet withholding funds, until the metadata records are accessible. In the case of data owned, governed and controlled by Inuit, First Nation, and Métis, the URs must provide information on the organization that will be storing, safeguarding, and managing the data emanating for their research.

8. Data Storage, Retention and Preservation

Researchers are not expected to deposit their data within a centralized ArcticNet repository.

[11] https://www.iso.org/standard/53798.html.
[12] https://www.fgdc.gov/metadata/geospatial-metadata-standards.
[13] http://dublincore.org/specifications/dublin-core/.
[14] Please note that this requirement does not apply retroactively to existing metadata records related to ArcticNet data.
[15] For further guidance, consult the UK Data Service (https://www.ukdataservice.ac.uk/ manage-data/document/metadata.aspx) or Cornell University (https://data.research.cornell.edu/ content/writing-metadata).
[16] Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. (2016). *The FAIR Guiding Principles for Scientific Data Management and Stewardship*. *Scientific Data, 3*(160018). https://doi.org/10.1038/sdata.2016.18.

ArcticNet is not structured for the long-term preservation of data. Individual projects are responsible for the identification of appropriate long-term repositories.[17] The choice of repository will vary across disciplines and data types, ranging from national or international, to institutional or discipline-specific repositories, however preference should be given to certified repositories that support open access where possible (such as Polar Data Catalogue[18], Nordicana D[19], Global Biodiversity Information Facility [GBIF],[20] Ocean Biodiversity Information System [OBIS],[21] or other domain-specific repositories supporting long-term preservation, digital object identifier [DOI] attribution and open access). Researchers are required to deposit into a recognized digital repository all data and metadata that directly support research results. The repository will ensure safe storage, preservation, and curation of data.

Plans for data storage (short-term or active), retention and preservation (long-term) should be considered during the early stages of project planning and be implemented throughout all stages of the project lifecycle. Measures may be taken to ensure data is preservation-ready, such as migration to preservation-friendly, non-proprietary file formats.[22] Data should be retained for as long as they are of continuing value to the stakeholder community, and as long as specified by the research funder, legislative, and other regulatory requirements. In many instances, stakeholders will resolve to retain research data for a period that exceeds the minimum requirement.[23]

To determine whether data should be preserved or archived, researchers should consider the data needed to validate research findings and results, and support replication and reuse, as well as the potential benefits that preserving and sharing the data long-term will have for their own or other fields of research, and for society at large. Researchers should also consider whether any ethical, legal, commercial, or cultural obligations prohibit sharing or preserving the data, and whether any de-identification or restricted access is required. Decisions and rationale for preservation and retention should be defined in the DMP.[24]

9. Data Access and Sharing

In accordance with the principles of this document, and with national and international best practices, ArcticNet data should be easily discoverable or findable and ultimately accessible, in addition to interoperable and reusable. While interoperability and reusability are enabled in part by use of rich metadata and domain-relevant community standards, discoverability or findability is enabled by ensuring

[17] For further guidance, consult the Registry of Research Data Repositories (re3data; https://www.re3data.org/) or the Portage Network Guide to *Repository Options in Canada* (2019; https://doi.org/10.5281/zenodo.3966349).
[18] https://www.polardata.ca/.
[19] http://www.cen.ulaval.ca/nordicanad/.
[20] https://www.gbif.org/
[21] https://obis.org/
[22] National Archives. (n.d.). *Digital File Types*. https://www.archives.gov/preservation/products/definitions/filetypes.html.
[23] Government of Canada. (2017). *Data Management Principles and Guidelines for Polar Research and Monitoring in Canada*. https://www.canada.ca/en/polar-knowledge/publications/data- management- principles-and-guidelines-2017-may.html.
[24] Government of Canada. (2015). *Tri-Agency Statement of Principles on Digital Data Management*. http://www.science.gc.ca/eic/site/063.nsf/eng/h_83F7624E.html.

metadata are published in an appropriate international, national, institutional, or subject-specific catalogue during the early stages of a project's life cycle, or listed in a central, publicly accessible index. Accessibility is enabled by making the data publicly available through an international, national, institutional, or subject-specific repository, or by documenting in an appropriate index a mechanism for access.

The use of persistent identifiers (PIDs), such as digital object identifiers (DOIs), also supports discoverability or findability and accessibility through uniquely identifying, and providing long-lasting reference to, data publications, research objects, researchers, and organizations.[25] As such, assigning globally unique and persistent identifiers to data and metadata further enhances FAIRness and maximises value and impact of ArcticNet research.[26]

Researchers have the right to benefit from the data they collect and generate, and as such all data users must provide appropriate citation, acknowledgement, or other attribution (when applicable, adhering to the request of the data originator) in any publications, presentations, or products arising from the use of the data.[27] In instances when formal citations are not possible, such as with some medical and social science data, the use of ethical policies for data collection and data use are recommended, such as those outlined in Article 8(j) of the 1992 United Nations Convention on Biological Diversity.[28]

10. Special Considerations for Data Access and Sharing

To support open access practices that maximize the benefit of proper data stewardship, researchers are encouraged to make data and metadata available fully, freely, and openly, with minimal delay. While data should be as open as possible, where ethical and legal considerations are present, it should also be as closed as necessary. The following exceptions to open access and sharing apply (adopted from the *Data Management Principles for Polar Research and Monitoring in Canada*[29]):

- where human subjects are involved or in situations where small sample sizes may compromise anonymity, confidentiality may be protected as appropriate and guided by the principles of informed consent and the legal rights of affected individuals;
- where Indigenous research and data is concerned, involving Indigenous and Local Knowledge, the rights of the knowledge holders shall not be compromised;

[25] Leggott, M., Shearer, K., Ridsdale, C.l, Barsky, E., & Baker, D. (2016). *Unique Identifiers: Current Landscape and Future Trends*. http://doi.org/10.5281/zenodo.557106.
[26] Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. (2016). *The FAIR Guiding Principles for Scientific Data Management and Stewardship*. *Scientific Data, 3*(160018). https://doi.org/10.1038/sdata.2016.18.
[27] Marine Environmental Observation Prediction & Response Network (MEOPAR). (2017). *Data Management Policy*. https://meopar.ca/wp-content/uploads/2021/01/Data_Management_Policy_ -_September_2017.pdf.
[28] Convention on Biological Diversity. (1992). Article 8(j): *Traditional Knowledge, Innovations and Practices*. https://www.cbd.int/traditional/.
[29] Government of Canada. (2017). *Data Management Principles and Guidelines for Polar Research and Monitoring in Canada*. https://www.canada.ca/en/polar-knowledge/publications/data- management- principles-and-guidelines-2017-may.html.

- where data release may cause harm or compromise security or safety, specific aspects of the data may need to be protected (for example, locations of nests of endangered birds or locations of sacred sites); and
- where pre-existing data are subject to access restrictions, access to data or information using this pre-existing data may be partially or completely restricted.

Any data access restrictions must be described and justified in a DMP based on these ethical, rather than proprietary, principles of data sharing. In cases where open public access may impede the researcher's right to benefit from the data they collect and generate, or where special considerations regarding data are present, such as the exceptions described above or further described in the following subsections, data may be stored privately for a time period of limited duration to allow for publication (i.e., an embargo), or may be stored privately indefinitely with access granted on an individual and limited basis. Access requests should identify the intended use of the data, how it will be handled, and how it will be cited, acknowledged or otherwise attributed. Such requests must be responded to and must not be unreasonably denied.[30]

10.1. Sensitive Data

As indicated by the exceptions listed in the previous section, certain types of data (e.g., data containing personally identifiable information [PII], Indigenous and Local Knowledge, or data related to commercially valuable or endangered species) may be considered sensitive, with the release of such data resulting in potential harms. The rights and privacy of individuals must be protected at all times. Any data made publicly available must therefore be free of PII and other variables that could lead to the deductive disclosure of the identity of individual subjects.[31] Any research and its corresponding data involving human subjects must conform to guidelines outlined in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2),*[32] and could involve the use of standard anonymization and access restriction procedures, and various institutional ethics review processes.[33]

10.2. Indigenous Research

Indigenous data, or those collected by governments and institutions about Indigenous Peoples and their languages, knowledge, practices, technologies, natural resources, and territories, are essential for Indigenous Peoples to exercise their individual and collective rights to self-determination and self-governance. Indigenous data sovereignty reinforces the rights to engage in decision-making in accordance with Indigenous values and collective interests. Research involving Indigenous data should adhere to community-generated research requirements, practices, and principles, such as the pan-

[30] Marine Environmental Observation Prediction & Response Network (MEOPAR). (2017). *Data Management Policy*. https://meopar.ca/wp-content/uploads/2021/01/Data_Management_Policy_ -_September_2017.pdf.
[31] Shearer, K. (2015). *Comprehensive Brief on Research Data Management Policies*. https://portagenetwork.ca/wp-content/uploads/2016/03/Comprehensive-Brief-on-Research-Data-Management-Policies-2015.pdf.
[32] Government of Canada. (2018). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2*. https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2018.html.
[33] For further guidance, consult the Portage Network's *Sensitive Data Toolkit for Researchers Part 2: Human Participant Research Data Risk Matrix* (https://doi.org/10.5281/zenodo.4088954).

Indigenous CARE Principles for Indigenous Data Governance, ensuring Collective Benefit, Authority to Control, Responsibility, and Ethics are thoroughly considered in collaboration with the Indigenous community involved in the research at hand.[34]

Supporting Indigenous data sovereignty and governance inherently includes support for First Nations, Inuit, and Métis Nation researchers, further brokering access, ownership and control over their research and their data. This support extends to building capacity for community-based data management practices, systems, and infrastructure where needed. First Nations, Inuit and the Métis Nation are best positioned to determine what information should be collected, how this information should be stored, analysed, monitored, used, shared, and preserved in ways that maximize benefits to communities while minimizing harm.[35]

For non-Indigenous researchers, Indigenous research must begin first and foremost with appropriate engagement of Indigenous peoples, communities or organizations throughout the entire data lifecycle, formal attribution of contributed knowledge, establishment of informed consent for use of knowledge and derived products, and the maintenance of contributor control of data.[36] This kind of engagement and consultation must occur first before any research is formally proposed, and, like the building of any meaningful relationship, will take time.

In accordance with Article 8(j) of the Convention on Biological Diversity (1992) concerning Traditional knowledge, innovations and practices,[37] researchers shall respect, preserve and maintain knowledge, innovations and practices of Indigenous and local communities embodying traditional lifestyles relevant for the conservation and sustainable use of biological diversity. In the context of Canada specifically, Chapter 9 of the *TCPS 2, Research Involving the First Nations, Inuit and Métis Peoples of Canada*[38] defines Indigenous Research as referring to primary research including:

- research conducted on First Nations, Inuit or Métis Nation lands in Canada and Indigenous lands worldwide;
- recruitment criteria that include Indigenous identity as a factor for the entire study or for a subgroup in the study;
- research that seeks input from participants regarding a community's cultural heritage, artefacts, knowledge or unique characteristics;
- research in which Indigenous identity or membership in an Indigenous community is used as a variable for the purpose of analysis of the research data or in the creation of survey tools; and
- interpretation of research results that will refer to Indigenous Peoples, lands, language, history and/or culture.

[34] GIDA. (2019). *CARE Principles for Indigenous Data Governance*. https://www.gida-global.org/care.
[35] Inuit Tapiriit Kanatami (ITK). (2018). *National Inuit Strategy on Research (NISR)*. https://www.itk.ca/wp-content/uploads/2020/10/ITK-National-Inuit-Strategy-on-Research.pdf. =
[36] International Arctic Science Committee (IASC). (2013). *The State of Principles and Practices for Arctic Data Management*. https://iasc.info/images/data/IASC_data_statement.pdf.
[37] Convention on Biological Diversity. (1992). Article 8(j): *Traditional Knowledge, Innovations and Practices*. https://www.cbd.int/traditional/.
[38] Government of Canada. (2018). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2*. https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2022.html.

While the CARE Principles and United Nations conventions, such as the Convention on Biological Diversity and the Declaration on the Rights of Indigenous Peoples (UNDRIP)[39], provide global pan-Indigenous frameworks, and Chapter 9 of the *TCPS 2* provides national Canadian guidance, the diversity and distinctions between First Nations, Inuit and the Métis Nation in Canada must be recognized and respected. Additional resources and guidance must be consulted based on the specific Indigenous Peoples, community, or organization the research concerns or will involve. For example, the First Nations Information Governance Centre (FNIGC) Principles of OCAP®, standing for Ownership, Control, Access, and Possession, clearly establish how First Nations data should be collected, protected, used, or shared.[40] The Inuit Tapiriit Kanatami (ITK) *National Inuit Strategy on Research (NISR)* similarly offers specific context and guidance on conducting research in Inuit Nunangat, identifying priority areas for advancing Inuit governance in research in support of self-determination.[41]

Required institutional ethics review processes will guide data management in these contexts, however Indigenous Peoples, governments, communities or organizations may have specific practices or requirements in place, and it is the responsibility of researchers to familiarize themselves with and adhere to these. These requirements may include storing and preserving data within the community, in which case researchers must opt for community-based repositories where possible, or writing data management, storage and long-term preservation capacity into funding applications to accommodate. Ongoing community consultation, engagement, and adherence to requirements builds respectful and meaningful partnerships that enhance the efficacy, impact, and usefulness of research for all involved or those it concerns.

10.3. Intellectual Property

Intellectual Property includes any data, model, improvement, invention or discovery, whether or not patented or patentable, all proprietary technical information, whether or not constituting trade secrets, and all copyrightable works, industrial designs, integrated circuit topographies, and trademarks, whether or not registered or registrable. Ownership shall be determined by the applicable Canadian Law. For further information on ArcticNet's Intellectual Property requirements, please see its Intellectual Property Policy.

Data made available to researchers by third parties is not subject to the data sharing requirements that are outlined in this policy. Researchers shall not enter agreements with a third party that would restrict the use or sharing of data collected or generated by ArcticNet-funded research. Data pertaining to Indigenous knowledge and data may be subject to additional sharing restrictions (see Section 10.2).

[39] United Nations (UN). (2007). *United Nations Declaration on the Rights of Indigenous Peoples*. https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf.
[40] First Nations Information Governance Centre (FNIGC). (2020). *The First Nations Principles of OCAP®*. https://fnigc.ca/ocap-training/.
[41] Inuit Tapiriit Kanatami (ITK). (2018). *National Inuit Strategy on Research (NISR)*. https://www.itk.ca/wp-content/uploads/2020/10/ITK-National-Inuit-Strategy-on-Research.pdf.

10.4. Ownership and Confidentiality

The researchers shall ensure that the appropriate agreements concerning the disclosure of Confidential Information and the transfer of biological and other materials are entered into prior to any disclosure of Confidential Information or transfer of material.

The data (or "Content") is provided by the researchers. ArcticNet does not warrant that such Content does not infringe the rights of any other person or entity. Furthermore, the researchers acknowledge that information or material which they provide electronically through their access to or usage of repositories or databases is not confidential or proprietary, except as may be required under applicable law, and acknowledge that unprotected e-mail communication over the Internet is subject to possible interception, alteration or loss. Trademarks and logos (collectively, "Marks") displayed on these repositories or databases are registered or unregistered Marks of the respective participating research programs, and are the property of their respective owner, and may not be used without written permission of the owner of such Marks.

10.5. Exclusion of Warranties

ArcticNet makes no representation or warranty regarding the functionality or condition of databases chosen by researchers, their suitability for use, or that their use will be uninterrupted or error-free. The databases and all their content are provided to the researchers "as is" without warranties of any kind. ArcticNet disclaim all warranties or conditions, written or oral, statutory, express or implied, including without limitation, no representation or warranty that (i) the content contained in or made available through the database will be of merchantable quality and fit for a particular purpose, (ii) the databases or their content will be accurate, complete, current, reliable, secure, or timely, (iii) that the operation of the databases will be uninterrupted or error-free, (iv) that defects or errors in the databases or the content, be it human or computer errors, will be corrected, (v) that the databases will be free from viruses and/or harmful components, and (vi) that communications to or from the databases will be secure and/or not intercepted. The Content is not intended to provide specific technical, business, accounting or other advice for the researchers' individual circumstances, and they should consult their own professional advisors to determine how any information or material provided on these Databases apply to their individual circumstances. These exclusions are in addition to any specific exclusion otherwise provided in these terms. To the extent that the jurisdiction to which the researchers are subject does not allow exclusion of certain warranties, such exclusions which are not permitted, do not apply.

Monitoring
Researchers are responsible for ensuring that project data are tracked and monitored on an ongoing basis and in a manner that is consistent with their data management plans.

Reporting
ArcticNet requires researchers to submit progress reports to their ArcticNet-funded project officer as part of their annual financial reporting. Specifically, researchers s are asked to indicate in their annual reports whether the project has encountered any data issues. If they have, researchers are required to summarize

in their project's annual progress report any data issues, how they were resolved, and any changes to their data management plans.

Security breach
Researchers and the participants involved in their project notify ArcticNet without undue delay and no later than twenty-four (24) hours upon becoming aware of a security breach. This notice shall minimally include a description of the:

- nature of the security breach, including, the type and number of data targeted by the security breach;
- likely consequences of the security breach on the data; and
- measures taken or proposed to be taken by researchers and the participants involved in their project to address the security breach, including, where appropriate, measures to mitigate possible adverse effects.

Once ArcticNet has received notification of a breach, it notifies its funders.

To the extent that such information is not available at the time of the notice to ArcticNet regarding said security breach, researchers and the participants involved in their project follow-up with ArcticNet as the information becomes available, in order to ensure full disclosure of the security breach without undue delay. The researchers and the participants involved in their project document responsive actions taken in connection with any security breach and conduct a post-incident review of events and actions taken.

10.6. Limitation of Liability

ArcticNet assumes no legal responsibility for the use of data provided by or held by ArcticNet researchers and expects all funded researchers to strive for the highest quality of data and metadata in their research. ArcticNet will not be liable for any damages, either direct or indirect, incidental, special or consequential, for use of or inability to use products or services of any kind, delay of or partial delivery, termination of rights or loss of profits, data, business or goodwill, whether on a contractual or extra contractual basis, or to provide indemnification or any other remedy to the researchers or any third party. The foregoing limitation shall apply even if ArcticNet knew of or ought to have known of the possibility of such damages. The researchers' sole and exclusive remedy is to discontinue using and accessing the repositories or databases. To the extent that the jurisdiction to which the researchers are subject does not allow any part of such limitation, such part does not apply.

10.7. Links

Links and references to other Internet websites are provided to the researchers as a convenience only. ArcticNet has not reviewed and does not expressly or impliedly endorse other Internet websites or any information or material, or the accessibility thereof, via such links, and does not assume any responsibility for any such other Internet websites, information or material posted thereon, or products or services offered thereon.

For More Information

Policies consulted when authoring this document:

Government of Canada. (2017). *Data Management Principles and Guidelines for Polar Research and Monitoring in Canada*. https://www.canada.ca/en/polar-knowledge/ publications/data-management-principles-and-guidelines-2017-may.html

Government of Canada. (2021). *Tri-Agency Research Data Management Policy*. http://www.science.gc.ca/eic/site/063.nsf/eng/h_97610.html

Government of Canada. (2015). *Tri-Agency Statement of Principles on Digital Data Management*. http://www.science.gc.ca/eic/site/063.nsf/eng/h_83F7624E.html

International Arctic Science Committee (IASC). (2013). *The State of Principles and Practices for Arctic Data Management*. https://iasc.info/images/data/IASC_data_statement.pdf

International Polar Year (IPY). (2006). *International Polar Year 2007-2008 Data Policy* http://ppsarctic.nina.no/files/ipy%20data%20policy.pdf

Marine Environmental Observation Prediction & Response Network (MEOPAR). (2017). *Data Management Policy*. https://meopar.ca/wp-content/uploads/2021/01/Data_ Management_Policy_-_September_2017.pdf

Memorial University (MUN). (2020). *Research Impacting Indigenous Groups Policy*. https://www.mun.ca/research/Indigenous/RIIG_Policy-2020.pdf

APPENDIX A

ARCTICNET DATA MANAGEMENT TEMPLATE FOR ULTIMATE RECIPIENTS

ArcticNet's Data Management Policy - Ultimate Recipients, which may be found here, outlines the data management requirements of Ultimate Recipients (i.e., project leads who signed funding agreements with ArcticNet). It requires Ultimate Recipients ("**URs**", each a "**UR**") to commit to ensuring that data management planning is undertaken at all stages of a project that involves data - from inception through to design and completion - and that data management plans are an essential part of this work.

ArcticNet has created this template for URs to complete in order to meet their data management requirements as specified by ArcticNet. The template guides URs through a series of questions and all of them must be addressed before their data management plan is considered complete. This template is based on the guidance provided through the Digital Research Alliance of Canada's Data Management Plan Assistant.

ArcticNet's data management-related monitoring and reporting requirements for URs may be found at the end of this document.

Data collection

1. What types of data will you collect, create, link to acquire and/or record (e.g., numeric, images, audio, video, text, tabular data, modelling data, spatial data, instrumentation data)?

2. What file formats will your data be collected in? Will these formats allow for data re-use, sharing and long-term access to the data?

Notes: Proprietary file formats requiring specialized software or hardware to use are not recommended, but may be necessary for certain data collection or analysis methods. Using open file formats or industry-standard formats (e.g., those widely used by a given community) is preferred whenever possible. Read more about file formats: Format: University of British Columbia (UBC) Library or Format Your Data: United Kingdom (UK) Data Service.

3. What conventions and procedures will you use to structure, name and version-control your files to help you and others better understand how your data are organized?

Notes: It is important to keep track of different copies or versions of files, files held in different formats or locations, and information cross-referenced between files. This process is called 'version control'. Logical file structures, informative naming conventions, and clear indications of file versions, all contribute to better use of your data during and after your project. These practices will help ensure that you and your team are using the appropriate version of your data and minimize confusion regarding copies on different computers and/or on different media. Read more about file naming and version control: Organize: UBC Library or Format Your Data: UK Data Service.

Documentation and metadata

1. What documentation will be needed for the data to be read and interpreted correctly in the future?

Notes: Typically, good documentation includes information about the study, data-level descriptions, and any other contextual information required to make the data usable by others. Other elements you should document, as applicable, include: the methodology used, variable definitions, vocabularies, classification systems, units of measurement, assumptions made, format and file type of the data, a description of the data capture and collection methods, explanation of data coding and analysis performed (including syntax files), and details of who has worked on the project and performed each task, etc.

2. How will you make sure that documentation is created or captured consistently throughout your project?

Notes: Consider how you will capture this information and where it will be recorded, ideally in advance of data collection and analysis, to ensure accuracy, consistency, and completeness of the documentation. Often, resources you have already created can contribute to this (e.g., publications, websites, progress reports, etc.).

It is useful to consult regularly with participants of the team to capture potential changes in data collection/processing that need to be reflected in the documentation. Individual roles and workflows should include gathering data documentation as a key element.

3. Are you using a metadata standard and/or tools to document and describe your data? If so, please list.

Notes: There are many general and domain-specific metadata standards. Dataset documentation should be provided in one of these standards, machine readable, openly-accessible formats to enable the effective exchange of information between users and systems. These standards are often based on language-independent data formats such as XML, RDF, and JSON. There are many metadata standards based on these formats, including discipline-specific standards.

Dataset documentation may also include a controlled vocabulary, which is a standardized list of terminology for describing information. Examples of controlled vocabularies include the Subject Headings: Library of Congress Subject Headings (LCSH) or NASA's Global Change Master Directory (GCMS) Keywords.

Read more about metadata standards: Disciplinary Metadata: Digital Curation Centre (UK)

Storage, backup, and protection

1. What are the anticipated storage requirements for your project, in terms of storage space (e.g., in megabytes, gigabytes, terabytes, etc.) and the length of time you will be storing it?

Notes: Storage-space estimates should take into account requirements for file versioning, backups, and growth over time. If you are collecting data over a long period (e.g., several months or years), your data storage and backup strategy should accommodate data growth. Similarly, a long-term storage plan is necessary if you intend to retain your data after the project has ended.

Please also note that to be in compliance with ArcticNet Data Management Policy for Ultimate Recipients (URs), confirm that your data as well as those of any participants involved in the project are hosted on servers located in Canada. You must also confirm that you are maintaining appropriate technical and organizational security measures to protect data from unauthorized loss, use, disclosure, alteration, or access and complying with any security measures that may be specified by their institution/organization and ArcticNet.

In addition, if you and any participants involved in your project are retaining the services of a service provider for the hosting of project data, the data must still be hosted on servers and facilities in Canada that are owned, controlled and operated by the service provider. You and any participants involved in your project must use reasonable efforts to ensure that the service provider is subject to information security controls at least substantially similar to those required under the UR agreement.

2. How and where will your data be stored and backed up during your project?

Notes: The risk of losing data due to human error, natural disasters, or other mishaps can be mitigated by following the 3-2-1 backup rule:

I. have at least three copies of your data;
II. store the copies on two different media; and
III. keep one backup copy offsite.

Data may be stored using optical or magnetic media, which can be removable (e.g., DVD and USB drives), fixed (e.g., desktop or laptop hard drives), or networked (e.g. networked drives or cloud-based servers). Each storage method has benefits and drawbacks that should be considered when determining the most appropriate solution. Further information on storage and backup practices is available from the Data Storage: University of Sheffield Library and Store Your Data: UK Data Service.

3. How will your team and other collaborators access, modify, and contribute data throughout the project?

Notes: An ideal solution is one that facilitates cooperation and ensures data security while also able to be adopted by users with minimal training. Transmitting data between locations or within project teams can be challenging for data management infrastructure. Relying on email for data transfer is not a robust or secure solution. Third-party commercial file sharing services (such as Google Drive and Dropbox) facilitate file exchange, but they are not necessarily permanent or secure, and are often located outside Canada. Please contact your library or data manager to develop the best solution for your project.

4. What measures will your team implement to protect the data from cybersecurity threats and how will you manage security breaches?

Notes: Ensure that your data management measures are aligned with your institutional/organizational cybersecurity policies and processes, as well as any cybersecurity requirements that may be specified by ArcticNet.

Please also note that to be in compliance with the ArcticNet's Data Management Policy for URs, you and the participants involved in your project must notify ArcticNet without undue delay and no later than twenty-four (24) hours upon becoming aware of a security breach.

This notice shall minimally include a description of the:

- nature of the security breach, including, the type and number of data targeted by the security breach;
- likely consequences of the security breach on the data; and
- measures taken or proposed to be taken by you and the participants involved in your project to address the security breach, including, where appropriate, measures to mitigate possible adverse effects.

Once ArcticNet has received notification of a breach, it must notify its funders, as per the requirements outlined in any funding agreements.

To the extent that such information is not available at the time of the notice to ArcticNet regarding said security breach, you and the participants involved in your project follow-up with ArcticNet as the information becomes available, in order to ensure full disclosure of the security breach without undue delay. You and the participants involved in your project document responsive actions taken in connection with any security breach and conduct a post-incident review of events and actions taken.

Preservation

1. Where will you deposit your data for long-term preservation and access at the end of your project?

Notes: The issue of data retention should be considered early in the project lifecycle. Data-retention decisions can be driven by external policies (e.g., funding agencies, business, journal publishers), or by an understanding of the enduring value of a given set of data. The need to preserve data in the short-term (i.e., for peer-verification purposes) or long-term (for data of lasting value), will influence the choice of data repository or archive. A helpful analogy is to think of creating a 'living will' for the data, that is, a plan describing how others will have continued access to the data.

If you need assistance locating a suitable data repository or archive, please contact your library. The directory re3data.org provides potential open data repositories. Verify whether the data repository will provide a statement agreeing to the terms of deposit outlined in your Data Management Plan.

2. How will you ensure your data is preservation ready?

Notes: Consider preservation-friendly file formats, ensuring file integrity, anonymization and de-identification, inclusion of supporting documentation. Some data formats are optimal for long-term preservation of data. For example, non-proprietary file formats, such as text ('.txt') and comma-separated ('.csv'), are considered preservation-friendly. The Format Your Data: UK Data Service provides a useful table of file formats for various types of data. Keep in mind that preservation-friendly files converted from one format to another may lose information (e.g., converting from an uncompressed TIFF file to a compressed JPG file), so changes to file formats should be documented.

Identify steps required following project completion in order to ensure the data you are choosing to preserve, or share is anonymous, error-free, and converted to recommended formats with a minimal risk of data loss. Read more about anonymization: Anonymize and De-identify: UBC Library or Data Protection: UK Data Service.

Sharing and reuse

1. What data will you be sharing and in what form? (e.g., raw, processed, analysed, final).

Notes: Raw data are the data directly obtained from the instrument, simulation, or survey.

Processed data result from some manipulation of the raw data to eliminate errors or outliers, to prepare the data for analysis, to derive new variables, or to de-identify the human participants.

Analysed data are the results of qualitative, statistical, or mathematical analysis of the processed data. They can be presented as graphs, charts, or statistical tables.

Final data are processed data that have, if needed, been converted into a preservation-friendly format.

Consider which data may need to be shared to meet your organization's, business' or funding agency's requirements, and which data may be restricted because of confidentiality/ privacy/intellectual property considerations.

2. Have you considered what type of end-user license to include with your data?

Notes: Licenses determine what uses can be made of your data. Your organization, business or funding agency may have end-user license requirements already in place; as may any data repositories where you may choose to store your data. If not, they may still be able to guide you in the development of a license. Once a license is created, please consider including a copy of your end-user license with your Data Management Plan. Note that only the intellectual property rights holder(s) can issue a license, so it is crucial to clarify who owns those rights.

There are a number of sources for examples/temples of a standard license template, such as the Creative Commons licenses and the Open Data Commons licenses. It can be easier to use a standard license rather than to devise a custom-made one. Note that even if you choose to make your data part of the public domain, it is preferable to make this explicit by using a license such as Creative Commons' CC0. For more information, read How to License Research Data: Digital Curation Centre (UK).

3. What steps will be taken to help others know that your data exists?

Notes: Possible tools for making data available to others include: data registries, repositories, indexes, word-of-mouth, publications.

4. How will your data be accessed (e.g., web service, file transfer protocol, etc.)?

Notes: One of the best ways to refer others to your deposited datasets is to cite them the same way you cite other types of publications (articles, books, proceedings). The UK Digital Curation Centre provides a guide for how to Cite Datasets and Link to Publications. Some data repositories also create links from datasets to their associated papers, thus increasing the visibility of the publications. Contact your library for assistance in making your dataset visible and easily accessible. There may be assistance available within your organization, business or funding agency to assist in making a dataset accessible.

If choosing a data repository, it would be beneficial to consider one that assigns a persistent identifier (such as a Digital Object Identifier (DOI)) to your dataset. This will ensure a stable access to the dataset and make it retrievable by various discovery tools.

Responsibilities and resources

1. Who will be responsible for managing this project's data during and after the project?

Notes: It is important to identify important data activities in your project and who will be responsible -- individuals or organizations -- for addressing these parts of your data management plan. This should include timelines associated with these team responsibilities and any training needed to prepare the team for these duties. For all ArcticNet data management reporting, UR must identify an individual who is the project's point-of-contact for all project-related activities and issues, including data management.

2. How will responsibilities for managing data activities be handled if substantive changes happen in the personnel overseeing the project's data, including a change of principal investigator?

Notes: Indicate a succession strategy for these data in the event that one or more people responsible for the data leaves. Describe the process to be followed in the event that the principal investigator leaves the project. In some instances, a co-investigator overseeing this project may assume responsibility.

3. What resources will you require to implement your data management plan? What is your estimate of the overall cost for data management?

Notes: This estimate should incorporate data management costs incurred during the project as well as those required for the longer-term support for the data after the project is finished. Items to consider in the latter category of expenses include the costs of curating and providing long-term access to the data. Some organizations, businesses, or funding agencies state explicitly the support that they will provide to meet the cost of preparing data for deposit. This might include technical aspects of data management, training requirements, file storage and backup, and contributions of non-project staff.

Ethics and legal compliance

1. If your project includes sensitive data, how will you ensure that it is securely managed and accessible only to approved participants of the project?

Notes: Consider where, how, and to whom sensitive data with acknowledged long-term value should be made available, and how long it should be archived. These decisions should align with any legal and organizational requirements and, where applicable, with the requirements of relevant ethics boards. The methods used to share data will be dependent on a number of factors such as the type, size, complexity, and degree of sensitivity of data. Outline problems anticipated in sharing data, along with causes and possible measures to mitigate these. Problems may include confidentiality, lack of consent agreements, or concerns about Intellectual Property Rights, among others. In some instances, an embargo period may be justified; these may be defined by organizational, business, and funding agency policies on data. Restrictions may be imposed by limiting physical access to storage devices, placing data on computers that do not have external network access (i.e., access to the Internet), through password protection, or by encrypting files. Sensitive data should never be shared via email or cloud storage services such as Dropbox.

Please also note that to be in compliance with ArcticNet's Data Management Policy for URs, you and the participants involved in your project confirm that you will anonymize and remove all information relating to an identifiable person from the data prior to performing your work over the course of the project or to sharing or transferring such information to other parties, including ArcticNet.

In addition, except as otherwise permitted or required by applicable law or regulation, you are required to ensure that you and your project team only: (i) collect and use data that constitute personal information for the purpose the data was provided; and (ii) retain data that constitute personal information for as long as necessary to fulfil your purposes for collecting the data, including for the purposes of satisfying any legal, accounting, or reporting requirements.

2. If applicable, what strategies will you undertake to address secondary uses of sensitive data?

Notes: Obtaining the appropriate consent from participants when sharing with individuals and teams outside of your project is often a legal requirement and, where applicable, an important step in satisfying the requirements of relevant ethics boards. The consent statement that you use should identify certain conditions clarifying the uses of the data by others. For example, it may stipulate that the data will only be shared for non-profit purposes or that the data will not be linked with personally identified data from other sources. Read more about data security: Data Protection: UK Data Service.

Please also note that to be in compliance with ArcticNet's Data Management Policy for URs, you and the participants involved in your project must represent and warrant that they have all the third-party consents, permissions and rights required by any applicable policies or laws to provide access, storage, use, reproduction, and sharing of its data.

3. How will you manage legal, ethical, and intellectual property issues?

Notes: Compliance with privacy legislation and laws, that may impose content restrictions in the data, should be discussed with the officer responsible for privacy requirements within your organization, business, or funding agency. Outline how compliance with applicable privacy laws and regulations will be achieved and what safeguards will be in place to protect privacy. Be sure to anticipate other related requirements such as export control laws.

In some cases, ethics boards are central to the process of managing data, especially when human participants are involved in a project. Include a description of any processes that the project has undergone with an ethics board, when applicable, and what the outcomes were in terms of requirements related to legal and ethical issues.

Establishing clarity on intellectual property data-related issues is also important. If applicable, include a description concerning licensing, and intellectual property rights to the data, including a description of any ownership structures for the collection, production and sharing of data. Document terms of reuse in line with the relevant legal and ethical requirements, as applicable (e.g., subject consent, permissions, restrictions, etc.). A data management plan must also acknowledge that all IP derived from data, including anonymized data, datasets, labelled data, representations, trained models and outputs, are subject to the commitments and requirements of ArcticNet's Intellectual Property Policy.

4. How will you ensure that data are collected and managed ethically regarding designated groups[42]?

It is recommended in ArcticNet's Data Management Policy for URs that you develop a self-identification process for members of designated groups that is culturally respectful and that ensures that participants feel safe in disclosing their identity(ies) and that their information is protected and used appropriately.

When working with data created in the context of research by and with First Nations, Métis, and Inuit communities, collectives and organizations, it is important to ensure the data are managed according to principles developed and approved by those communities, collectives and organizations, and in partnership with them.

[42] The federal Employment Equity Act identifies the following as designated groups: women, people with disabilities, Indigenous peoples, and visible minorities.

Monitoring and reporting requirements

Monitoring

As a UR, you are responsible for ensuring that project data are tracked and monitored on an ongoing basis and in a manner that is consistent with your data management plan.

Reporting

In their annual progress reports submitted to ArcticNet, URs are required, after the first year of receiving ArcticNet funds, to provide links to their metadata records that have been submitted to recognized data repositories or metadata storing facilities. Failure to submit openly accessible metadata records will lead to ArcticNet withholding funds, until the metadata records are accessible. In the case of data owned, governed and controlled by Inuit, First Nation, and Métis, the URs must provide information on the organization that will be storing, safeguarding, and managing the data emanating for their research.

URs will also be asked to indicate whether the project has encountered any data issues. If it has, they are then asked to suggest solutions for addressing them and to report on their resolution in the subsequent progress report. In addition, URs are required to summarize any changes to their data management plan.

ArcticNet project officers will be responsible for notifying the Directors if any of the project's data issues or changes to the data management plan merit consideration at a higher level. The directors will oversee actions for resolving notable data issues to ensure the project is in compliance with ArcticNet's data management requirements.