Policy Number:	Policy Name: Research Data Management and Access Policy
Policy Revision Dates:	Page: 1

X-XXX Research Data Management and Access Policy

Through the 2013 memo from the Office of Science and Technology Policy, US federal funders were directed to institute policies to make broadly available with the fewest possible restrictions data, code and other research outputs. In alignment with these public access mandates, as well as commitments from ABOR universities towards the open access of scholarly articles, ABOR is committed to increasing access to research data for the people of Arizona and the world. Separately, ABOR recognizes that good data stewardship is needed not only to support these efforts, but also for compliance with data retention and security regulations. ABOR requires Arizona's public universities to create and implement the necessary local processes and standards to effectively govern research data, as defined in this policy.

Each institution shall:

1. Designate an appropriate office responsible for the policy (e.g., the research office, office of the vice-president for research, etc.). The responsible office will designate an advisory group consisting of at least the institutional units/offices ultimately responsible for supporting compliance with this policy. The advisory group will develop and review the policy in consultation with other relevant stakeholders at an interval of no more than 3 years.
2. Build upon or reference existing policies and regulations where possible (e.g. The ABOR Intellectual Property Policy, institutional data retention policies, etc.)
3. Aim to ensure robust, trustworthy, and ethical data stewardship practices while fostering a culture that encourages and guides researchers toward making data "as open as possible and as closed as necessary."
4. Implement mechanisms (e.g. data management plans, process controls) that allow tracking compliance with the policy to the extent that is practicable.

Definitions of capitalized terms are included in the final section of this policy.

A. Policy Owner
   1. This policy is defined and owned by the Arizona Board of Regents (ABOR). ABOR requires each university to designate an institutional Research Data Steward as the responsible party for oversight, implementation, maintenance, and periodic review of the local compliance with this policy.

B. Review Period
   1. The Research Data Steward will coordinate a periodic review of the local processes and controls in consultation with other relevant stakeholders at a maximum interval of 3 years. In order to conduct the review, the Research Data Steward is responsible for convening and chairing an advisory group consisting of at least the institutional units/offices ultimately responsible for supporting compliance with this policy.

C. Who Does This Policy Apply To?
   1. This policy applies to:
      a. Any Researcher overseeing or performing research conducted at or under the auspices of ABOR universities when research data are collected or produced, regardless of the source of funding.
      b. Any individual who has been designated as a Research Data Manager under this policy.

c. Any individual who has been designated as a Research Data Steward under this policy.

2. Exceptions:

a. Students are excepted when the research data are collected or produced as part of credit-bearing coursework or internships.

D. Data Stewardship & Governance

1. Data Ownership

a. Ownership of Research Data is governed by the ABOR intellectual Property Policy. For the avoidance of doubt regarding Research Data ownership

b. Research Data is considered as Tangible Research Property under the ABOR Intellectual Property Policy

c. Research Data produced under the auspices of an ABOR university is the property of ABOR unless ownership is altered under the exceptions specified in the ABOR Intellectual Property Policy.

2. Researcher Responsibilities

a. The Principal Investigator shall:

(1) Designate one or more Research Data Managers (RDM). The Principal Investigator can designate themselves as the RDM.

(2) Ensure that the designated manager(s) understand and are able to comply with any applicable policies and regulations.

(3) The identity of the manager(s) will be recorded in documentation stored with the data or in a Data Management Plan.

(4) Ensure that an understandable and usable copy of the data remains accessible at the institution under the management/stewardship of a designated individual(s) or unit(s) for the purposes of compliance with the other sections of this Research Data Management and Access Policy.

(5) Attempt to resolve any questions, conflicts, or concerns by contacting the appropriate institutional office.

3. Institution Responsibilities

a. The relevant ABOR university shall:

(1) Comply with regulations and the terms of all grants and awards as they pertain to Research Data.

(2) Institute mechanisms at appropriate administrative points in the research data lifecycle (e.g., grant submission, reporting, project completion) in order to communicate the existence of this policy and assist projects to comply through review and sharing recommended practices.

(3) Communicate to Researchers the institutional resources available for support in complying with elements of this policy, including retention, access, security, and the development of data management plans.

(4) Ensure that relevant units and offices evaluate which points within their workflows are most appropriate to promote the availability of institutional research data support and, when appropriate, coordinate with one another to assist Principal Investigators in complying with this Policy.

E. Data Management Practices
   1. Metadata
      a. Research Data should be documented to the degree necessary to ensure that an investigator not involved with the research can correctly interpret the data. In general, a metadata standard appropriate to the field of research should be considered for documenting data unless the Research Data Steward determines that standard to be inadequate to meet the needs of the institution.
   2. Data Storage
      a. Research Data should be stored in an environment that provides the security and data resilience appropriate for the type of data associated with the research.
   3. Requirements for Sensitive and Regulated Data
      a. Conducting research with Sensitive or Regulated Research Data has legal and ethical implications with respect to the collection, storage, publication and preservation of these data. Therefore, all Researchers conducting research of a sensitive nature are required to:
         (1) For human subjects Research Data, obtain the appropriate informed consent for information sharing from participants prior to collecting and analyzing the data,
         (2) Choose a university-approved storage medium that satisfies security requirements for the data,
         (3) Ensure that anonymization and access to the data are appropriately controlled,
         (4) Meet all contractual obligations required by third party data sharing agreements
         (5) Monitor and manage data security and legal and ethical obligations at all times when working with sensitive data,
         (6) Appropriately assess which information can be published at study completion,
         (7) Use protocols to protect locations of sensitive environmental or archaeological data,
         (8) Not release Research Data if it contains confidential or proprietary information. Research Data must be properly de-identified or anonymized prior to sharing.
         (9) Not release Research Data if prohibited by contractual or license agreements.
      b. The steps that will be taken to protect the data during the life of a research study should be clearly documented in the Data Management Plan and the Principal Investigator is responsible for ensuring these provisions are respected. Consult the University's research data protection guidance for additional, detailed information regarding research data involving human subjects and the rights of participants rights and the interests of Researchers.
   4. Data Use Agreements
      a. Research that requires acquiring or sharing research data may be governed by a Data Use Agreement. University researchers are not permitted to enter into Data Use Agreements as individuals. If a Data Use Agreement is required, the researcher should contact the appropriate university department to facilitate negotiations and signature with the external organization.

F. Data Access and Availability
   1. Public Access

a. Public access to Research Data lowers the barrier to building on the research produced at ABOR institutions. This ensures Arizona's universities comply with mandates from federal funders and are also recognized as major contributors to cutting edge research and innovation.
    (1) In order to meet contractual obligations from federally funded research, this policy requires making available the final Research Data no later than 2 years after the end of the funded period, unless a different period is mandated by the terms of an award or contract. For Research Data supporting peer-reviewed publications, these will be made available at the time of publication or according to the journal's requirements.
    (2) The requirements from A) will extend to any Research Data produced under the auspices of ABOR universities regardless of funding source (e.g., data resulting from internal grants, seed funded work).
    (3) Public access compliance is achieved when materials are included with a peer reviewed article as supplementary information and/or are deposited in an institutional data repository or third-party repository intended for long-term data availability. Placing materials solely on personal or professional websites or on platforms not intended for or unable to support long-term access (e.g., Google Drive, Github) is not sufficient to comply with this requirement.
    (4) Research Data Stewards who give other Researchers access to Research Data must inform them, in writing where appropriate, of any limitations or restrictions on the use or dissemination of the data. Examples of how this may be achieved include but are not limited to the use of established licenses (Creative Commons, GNU, MIT) or data use agreements.
    (5) These public access requirements will not apply if they are superseded by specific provisions in contracts and awards, to any materials not subject to this Research Data Policy, or materials that cannot be made publicly available due to their nature.

2. Administrative Access and Availability
    a. Researchers must retain access to Research Data resulting from research projects they themselves have initiated, and to Research Data acquired by processes for which they were primarily responsible.
    b. Research data are to be accessible to members of the University community, external collaborators and others as appropriate (e.g., for patent applications or journal submissions). Where necessary to assure needed and appropriate access (e.g., for research misconduct investigations), the University may take custody of Research Data in a manner specified by the Vice President for Research.
    c. Research Data are to be retained according to institutional data retention policies.
3. Data Retention
    a. Federal regulations require research records to be retained for at least three years after the completion of the research (45 CFR 46). This policy additionally requires that the Research Data, associated Metadata and any other relevant documentation be retained

for a minimum of seven years. Additional funder requirements may supersede this requirement, depending on the field of study. Research involving Personally Identifiable Health information (PHI) is subject to HIPAA regulations. These regulations require data to be retained for at least six years after participant authorization. Some research sponsors may specify longer retention periods. Regardless of these minimum retention periods, it is advisable to retain the data for as long as is practical in order to be able to support the results obtained and presented in publications.

b. Assuming all research records are stored appropriately, Research Data, associated Metadata and any other relevant documentation can be retained indefinitely, although this practice must be balanced against the cost of archival storage and other considerations. Studies involving human subjects should abide by the retention schedules included in the Informed Consent completed by study participants.

c. All research projects should explicitly state the retention period in the Data Management Plan.

d. Publication of Research Data and Metadata in an appropriate long-term data repository may alleviate the need for local storage of some data. If that is the case, documentation should exist that identifies what data were published and where these data reside.

4. Data Management Costs

a. Many funders consider data management costs a legitimate grant expense. Storage and other data management expenses should be budgeted for, including the cost of preservation, unless an explicit commitment is made by the university to provide these resources as in-kind support. Researchers should consider the cost of management and publication of research data, both during and after the project. These expenses should be viewed through the same lens as those associated with manuscript publication. These projected costs should be quantified and included in the proposal submission, if appropriate.

b. Institutions should be prepared to quantify the technology and personnel costs associated with effective research data management, publication and preservation and provide these as budget line items in support of proposal submissions. It is recommended that a proposal budget should, at a minimum, include funds for the data retention period required by the funding agency.

G. Ethics in Data Use & Reuse

1. Research data publications should include an ordered list of contributors with reference to their role in the development of the dataset; contributors may be independent of other related publications and therefore should take proactive steps to ensure contributor credit in publishing research datasets with the recognition that datasets are standalone published works distinct from other research outputs.
2. Principal Investigators are responsible for considering ethical implications of data use and for including any reuse restrictions. To ensure they are not submitting any datasets that should not be made openly available to the public, full consideration includes review of policies for sensitive and regulated data and institutional policies as well as evolving community norms and recommended practices. Institutional research data repositories will provide and enact

policies informing depositors of potential actions if they violate any agreements between their IRB, community partners, or subjects of their research. They will also provide data use agreements where necessary that inform uses of how Research Data can be used if there are any restrictions.

H. Researcher Departure from ABOR Universities

1. Researchers leaving their university are expected to meet with their respective research administration service provider to take steps to ensure continuity of projects, transfer of grant to new institution, appointment of an alternative Principal Investigator, termination of project, or other changes of investigator to take ownership of research dataset management and sharing responsibilities as appropriate to their project and agreements.
2. If a Principal Investigator leaves, data ownership may be transferred to another institution with the approval of the applicable academic or research unit who shall determine who will take stewardship (see definitions) in consultation with the Vice President for Research. The Principal Investigator may take copies of research data for projects on which they have worked. The purposes for which such data may be used are subject to relevant confidentiality restrictions, or as formally agreed-upon beforehand in a data use agreement. The original or primary Research Data must be retained at the university unless the Vice President for Research specifically authorizes moving it to another institution.
3. If a Principal Investigator leaves the University and a project is to be moved to another institution, ownership of the data may be transferred with the approval of the Vice President and Associate Provost for Research, and with written agreement from the new institution that guarantees: 1) its acceptance of custodial responsibilities for the data, 2) University access to the data, should that become necessary, and 3) relevant confidentiality restrictions, where appropriate.
4. If a student or researcher leaves the institution, the Principal Investigator shall determine who will take stewardship (in consultation with Assoc. VP for Academic Programs, if student).

I. Data Management Plans

1. The creation of a Data Management Plan (DMP) by the Principal Investigator prior to beginning a research project is encouraged but not required UNLESS one of the following is true:
   a. It is required by an external funder.
   b. The research is being funded internally by ABOR or by an ABOR university.
   c. Substantial university resources are being committed as part of the work (see below the list of services that trigger this requirement).
   d. There is a significant legal or financial risk to the institution if the research data were to be lost or inadvertently released.
2. DMPs for External Awards and Contracts
   a. Principal Investigators are required to comply with any DMP requirements set forth in awards and contracts. In the event of a conflict, the terms of the award or contract shall supersede the conflicting element in this Policy.

b. In any DMP, Principal Investigators must state how they plan to comply with this Policy. If any institutional resources are being committed as part of the DMP, they must be listed and, where appropriate, a statement of support from the appropriate unit or office.

3. DMPs for Internal Awards
   a. For any grants awarded by ABOR institutions, the granting office or unit will require applicants to submit a data management plan as part of the application packet.
   b. The plan shall be factored into granting decisions.
      (1) Criteria for assessing the adequacy of the plan shall include evaluating compliance with this Research Data Policy.
      (2) The format and contents of the plan is at the discretion of the unit. However, it is recommended to align with federal funder requirements such as those laid out by the National Science Foundation (PAPPG Part I Chapter II C.2.j) or other appropriate standards.
   c. In any DMP, Principal Investigators must state how they plan to comply with this Policy. If any institutional resources are being committed as part of the DMP, they must be listed and, where appropriate, a statement of support from the appropriate unit or office.
4. Institutional Services that must be Included in a DMP

1. If any of the following institutional services are anticipated to be used at any point during or after the award or contract period, they must be included in a DMP. To ensure needs can be met, Principal Investigators are strongly encouraged to engage with the service provider unit during proposal development.
   a. Specialty compute resources (e.g., high performance computing resources, departmental servers or other IT services beyond those normally provided to all students, faculty, and staff)
   b. Specialty research tools or environments used in Research Data production, manipulation, or management (e.g., HIPAA-compliant or CUI-compliant servers, big data storage supported by the institution, specialty software products or equipment such as 3D scanners, 3D printers, virtual reality, visualization walls, or any core facility)
   c. Research Data archiving services (e.g., institutional data repositories, curation services)
   d. Any consulting services requested from units that explicitly provide data support services (e.g., university IT, research computing, de-identification, library data services)

J. Definitions

1. “Code” means the combination of data and computer executable instructions that when combined may be used to manage, analyze, model or manipulate research data.
2. “Data Management Plan (DMP)” is a document, typically submitted in support of a grant application, that describes how data will be collected, processed, documented, stored, published and preserved as part of a research cycle.
3. “Data Use Agreement” is a contractual agreement used to define how access to and/or exchanged data may be used. The primary consideration is the protection of: protected health data (PHI) in accordance with HIPAA Regulations, personally identifiable information (PII) or other proprietary, commercial information. However, DUAs can be used in other situations

where the exchange of data is necessary and an agreement detailing the responsibilities of both parties is required.

4. “Intangible Property” is as defined in the ABOR Intellectual Property Policy, i.e. “property having no physical existence, such as trademarks, copyrights, patents and patent applications and property, such as loans, notes and other debt instruments, lease agreements, stock and other instruments of property ownership,” and includes research data.
5. “Investigator” is the person, whether as an employee, or otherwise affiliated with a university, whose position, responsibility statement, job description, employment assignment and/or function within the university is, either in whole or in part, to carry out research, whether sponsored by external sources, internal sources, or are unfunded. Such investigators shall include, but not be limited to, faculty, staff, other paid employees, or other individuals supported with university funds. See also Researcher and Principal Investigator.
6. “Metadata” means the accompanying information, either in a separate file or otherwise combined with the Research Data that sufficiently describes the data to facilitate re-use and avoid misinterpretation. Metadata will include, but is not limited to, an author’s name, publishing date, title of data contents, description of contents, research methods and other such related information.
7. “Policy Owner” is the Arizona Board of Regents and any ABOR employee who has the assigned responsibility for managing the periodic review of this policy on behalf of the Board of Regents.
8. “Principal Investigator (PI)” is an Investigator who has primary responsibility for a research project within the university for the design, conduct and reporting of research.
9. “Project Closeout” applies when 1) a sponsored project award period has ended, and all deliverables have been submitted, or 2) non-sponsored project work has ended, and no further publications related to the project are anticipated.
10. “Researcher” is any faculty member, student, postdoctoral researcher, research associate or fellow, or other person involved in the design, conduct or reporting of research. See also “Investigator”.
11. “Research Data” is defined as any recorded material collected, retained, and accepted by investigators in the course of a research project that are also used to derive and validate research findings. Research Data include both derived data (e.g., statistics, findings, formulas, etc.) and primary physical and digital data (e.g., notebooks, protocols, images, case history records, etc.). Research data may be quantitative in the form of spatial and tabular files, remote sensing output; qualitative information such as documentation, interviews, and survey results; and supplementary information including images, digitized physical samples, audio of video recordings, computational models or other relevant software/code.
12. “Research Data Manager” is the assigned employee (faculty or staff) who has responsibility and decision-making authority for the documentation, management, sharing, and security of the Research Data collected, stored and ultimately published as part of a research study.
13. “Research Data Steward” is the assigned employee (faculty or staff) who has responsibility and decision-making authority for the local implementation of this policy, including the controls

(processes and tools) that support the documentation, management, sharing, and security of the research data collected, stored, and ultimately published at the institution.

14. “Sensitive Data” is any Research Data that requires additional protections to ensure the information collected is not compromised through mishandling. Sensitive Data may include: human subjects research data containing Personal Identifying Information (PII) or Protected Health Information (PHI), data acquired through purchase and restricted by license agreement from publication, confidential data where a Data Use Agreement (DUA) restricts publication, environmental data where disclosure of location or similar information would place populations of rare or endangered species at risk, culturally sensitive (e.g. archaeological) data that may require similar protections, or any data, that if released, would potentially harm an individual, or community, or have a significant negative public impact, if disclosed.
15. “Substantial University Resources” are the resources provided by the university that go above and beyond what is customarily provided to university employees or students. Substantial Resources will vary by university, department/unit, and context. To be substantial the resources must be beyond the ordinary (e.g. computer) and must be more than what other members of the department or students in similar situations are regularly offered as support for their work.
16. “Tangible Research Property” are the items produced in the course of research, such as compositions, chemical compounds, biological materials, materials, drawings, devices, integrated circuit chips, computer databases, computer software, prototypes, circuit designs, and equipment.” Tangible Research Property shall be treated as research data only to the degree that it meets the definition of Research Data above, or when funding agency regulatory or contract language requires that it be classified as such (e.g. the use of physical samples or images to support findings in published papers).