



NORTHWEST FOUNDATION, INC.

NORTHWEST MISSOURI STATE UNIVERSITY

Policy Name:	Data Governance Policy
Effective Date:	April 23, 2021
Foundation Board President Signature:	<i>Robert Russell</i>
Executive Director Signature:	<i>Melissa Marchant</i>

Data Governance Policy

1. Statement of Purpose

Northwest Foundation data are assets maintained to support the Foundation's central mission to develop and steward philanthropic resources for the benefit of Northwest Missouri State University and its students. To support the effective pursuit of philanthropy support, Foundation data must be accessible to University Advancement staff and certain University personnel while maintaining a high level of donor privacy.

The purpose of the Data Governance Policy is to:

- Ensure proper access by Advancement staff and other University personnel
- Improve the security of the data, including privacy, confidentiality and protection from loss
- Improve the integrity of the data resulting in great accuracy, timeliness and quality of information

2. Data Governance RACI (Responsible, Accountable, Consulted, Informed)

Responsible	Information Security Coordinator –CFO
Accountable	Northwest Foundation Governance Committee
Consulted	Associate Vice President of Information Technology Cyber security sub-committee of Northwest Foundation board Database Administrator
Informed	University Advancement Staff Northwest Foundation board of directors Northwest Missouri State University leadership team

3. Data Inventory

See Addendum

4. Information Security Classification

With regard to the data elements collected per the above inventory, Personal Identifiable Information (PII) means either a constituent's name in combination with any one or more of the following data

elements: social security number, federal ID number, date of birth and credit card numbers. Sensitive information includes: race, ethnicity, gift history and possibly some documented communications. Contact information is considered publically available information.

5. Data Access

The purpose of a data access plan is to ensure employees have appropriate access to Foundation data and information. The value of data as a resource is increased through appropriate use and diminished through misuse, misinterpretation and unnecessary restrictions to its access. While recognizing the Foundation's responsibility for the security of data, the procedures established to protect data should not interfere unduly with the efficient conduct of Foundation business.

The Foundation will protect its data ensuring that third party vendors adhere to appropriate security measures and through other security measures (user IDs, passwords, encryption, computer & network security) that assure the proper use of data when accessed. University Advancement staff and other University personnel shall be granted access to Foundation data on a need to know basis as determined by the Information Security Coordinator. Access to PII and sensitive information will be more limited than that of contact information.

6. Data Usage

The purpose of the data usage policy is to ensure that Foundation data are not misused or abused, and are used ethically with due consideration for individual privacy. Advancement staff and other University personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes. Data usage falls into three categories: update, read-only; and external dissemination.

Authority to update data shall be granted by Information Security Coordinator only to personnel whose job duties specify and require responsibility for data update.

Read-only usage will be granted to advancement staff and other university personnel for the support of Foundation business.

Only data elements not designated as PII or sensitive data may be externally disseminated. Even the release of such information should be guided by the need to respect individual privacy and protect the integrity of the data. The release of all other data must be approved by the Information Security Coordinator.

7. Data Integrity and Integration

Data integrity refers to the validity, reliability, and accuracy of data. Data integrity relies on a clear understanding of the business processes underlying the data and the consistent definition of each data element. Data integration is the assimilation of data into information systems.

To ensure that Foundation data have a high degree of integrity and that key data elements are integrated into appropriate information systems, the Database Administrator in conjunction with the Information Security Coordinator shall develop procedures manuals which define each key data element and the business processes underlying the data.

Other related documents

- Record Retention Policy
- Risk Management Assessment Policy
- Written Information Security Program
- Incident Response Plan
- Software and Technology Provider Assessment
- Northwest Foundation Privacy Policy
- Northwest Missouri State University Technology policies:
<https://www.nwmissouri.edu/compserv/privacy-policies.htm>

Data Governance Policy Addendum – Data Inventory

Our alumni and friend database as well as our financial system software is hosted by Blackbaud in their Financial Edge and Raiser's Edge software solutions.

The Financial Edge includes general ledger, fund accounting tracking, cash management and accounts payable functions. With the exception of certain vendors for which we maintain their social security number or federal ID number, data is highly summarized and does not include any sensitive or personally identifiable information.

The Raiser's Edge database is a comprehensive collection of information from which subsets of data are pulled to be used in other software solutions such as spreadsheets for mailings or further analysis or call center software.

Types of data collected in The Raiser's Edge (not all records have all data elements):

- Contact Information: address, phone, email address, social media accounts
- Demographic Information: race, ethnicity, gender, age, birthdate, marital status
- Relationships: parents, children, relatives, friends
- School information: degrees, majors/minors, school activities, class year, other institutions attended, scholarships received
- Employment history: job title, employer, location
- Financial information: gift history, credit card number (encrypted and obscured)
- Communications: meetings, calls and emails between constituent and Northwest employees may be documented
- Volunteer activities: activities conducted on behalf of the University or the affiliates
- Engagement activities: interaction with the University or affiliated organizations in meetings, groups, events or social media
- Other information: other information you provided us in the process of conducting business with Northwest or obtained from other publically available sources

The Foundation collaborates with Northwest's office of financial assistance and scholarships to provide a standardized scholarship application utilized by current and prospective students. The software solution Scholarship Manager by NextGen collects a significant amount of FERPA (Federal Educational Rights and Privacy Act) protected data from both University systems and applicants. The University's privacy policy documented at <https://www.nwmlsso.uri.edu/comperv/privacy-policies.htm> covers data collected from students for the purposes of financial assistance.