

WESTERN NEBRASKA COMMUNITY COLLEGE

Western Community College Area Board of Governors' Policy

TITLE: Data Governance

DIVISION: General Institutional

CATEGORY: Records/Information

REFERENCE: Family Educational Rights and Privacy Act (FERPA)
20 U.S.C. § 1232g; 34 CFR Part 99; and 34 CFR §99.31;
U.S. Department of Education Program Participation
Agreement (PPA) and the Gramm-Leach-Bliley Act
(15 U.S. Code § 6801)
Nebraska Revised Statute(s): §79-776; and §85-1511;

NUMBER: BP-702

APPROVAL/DATE: F. Lynne Klemke, Chair, WNCC Board of Governors
Date: January 15, 2020

Purpose:

Data is a critical component in the decision-making process at Western Nebraska Community College (WNCC). Data elements should be collected and utilized not only for operational purposes, but also for analysis, control, and strategic decision-making. To maximize effectiveness, mechanisms must be developed to collect, safeguard, and distribute accurate, consistent, and useful information to appropriate members of the WNCC community.

WNCC shall develop a data governance framework to focus on creating procedures and guidelines on appropriate data stewardship and strategies. The institution, in compliance with WNCC Board Policies and expectations, shall continue its efforts to promote, communicate, and train the College community on proper data practices with a goal of continuous quality improvement.

Scope

This policy governs all aspects of the College. All WNCC employees who use data, regardless of the form of storage or presentation, shall abide by this policy. All senior administrators have the responsibility to understand and implement this policy, including, as necessary, the adoption of specific procedures for their respective areas in furtherance of and in accordance to this policy.

Definitions

Data Element: A single data item (i.e., a last name is a data element).

Data Dictionary: A reference tool which provides a description of all the core institutional data elements.

Data Dissemination: The distribution of data to either internal or external stakeholders. Included in dissemination is the sending of data to external entities including vendors that provide services for WNCC.

Data Integrity: The qualities of reliability and accuracy of data values that permit the institution to have dependable data on which to make plans, projections and decisions. Data integrity contributes to the efficient operation of the institution by supporting quality customer service to students, faculty, and employees and helping the institution remain competitive.

Data Integration: The ability of data to be assimilated across information systems is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

Data Model: A diagrammatic representation of the objects and their properties that are needed within an organization to accomplish its mission. Sometimes represented as an ER (entity-relationship) diagram or a data flow diagram.

Data Steward: Managers of functional areas of Colleague (typically at the level of Registrar, Director of Admissions, Director of Human Resources, etc.) who oversee the capture, maintenance, and dissemination of data for a particular operation. Data stewards are responsible for making security decisions regarding access to the data under their purview.

Data Value: The set of values that each data element can have. For example: numeric or alpha for academic departments (i.e. ACCT or ENGL).

Institutional Data: The data elements that are aggregated into metrics relevant to operations, planning, or management of any unit at WNCC; that are reported to the WNCC Board of Governors, federal, and state organizations; generally referenced or required for use by more than one organizational unit; or included in official administrative reporting.

Policy

The institution will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant Data Steward to have an appropriate access level. WNCC will provide the technology framework for data access to be provisioned. The Data Stewards are responsible for ensuring the access levels are appropriate and that proper training is provided to the employee prior to authorizing data access. Read-only access to administrative information may be provided to employees for the support of institutional business without unnecessary difficulties/restrictions.

Institutional data must be safeguarded and appropriate protocols, including creation and maintenance of a data dictionary, shall be required to ensure such data is used in an ethical

manner, according to any applicable law, and with due consideration for individual privacy. Use of data depends on the security levels assigned by the Data Steward. WNCC personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate and unethical purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of update and dissemination.

Authority to update data that is reported as key institutional data shall be granted by the appropriate Data Steward only to personnel whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with WNCC's desire to provide excellent service to faculty, staff, students, and other constituents. Data Stewards shall ensure that adequate internal controls and/or change management procedures are in place to manage 'updates' to key institutional data, their definitions and processes.

Data dissemination must be controlled in accordance with the security practices set forth by the Data Stewards. These security practices shall be in accordance with the data model or decision flow chart that shall be created and maintained by the WNCC ERP Governance Committee. Appropriate use must be considered before sensitive data are distributed.

Unauthorized dissemination of data to either internal/external personnel shall constitute a violation of this policy. Appropriate disciplinary measures shall be taken, which may include termination of employment and/or criminal prosecution.

The need for data integration is critical. Therefore, maintaining the integrity of the data and developing a data model which corresponds to data structures and domains is vital. Therefore:

- There shall be no downloading of individually identifiable data from central systems to electronic files for the purpose of uploading or connecting the data to non-central systems (e.g., shadow systems, external vendors) without the knowledge of the Information Technology Department. This practice introduces risks associated with data integrity, security, and long-term sustainability of information systems that may not be mitigated due to the nature of the practice. Departments and/or personnel responsible for these practices that are found to be in violation of this policy, may result in disciplinary actions up to and including dismissal from employment consistent with WNCC Board Policy and WNCC Presidential Procedures.
- Approval by the Data Steward is specific to each request. Data granted for one purpose is not universally granted for all purposes. Each new use case must be approved by the Data Steward in a new request or an amendment to the original request. Documented agreements regarding data use, retention, and responsibility should exist with the Data Stewards (and vendors in the case of data integration with external entities) of the systems providing and utilizing data. Data extraction practices that are already in use should be registered and documented agreement developed with the appropriate Data Steward member.

- Data systems and/or processes that are involved in the creation of institutional reports should incorporate data integrity and validation rules that ensure the highest levels of data integrity are achieved. Data verification programs such as consistency and reasonableness checks shall be implemented to identify data tampering, errors, and omissions.

Revising this Policy

This WNCC Board policy supersedes any prior WNCC policy, procedure, guideline or handbook on this subject matter.

If statutory provisions, regulatory guidance, or court interpretations change or conflict with this Board Policy, the Board retains the right to revise accordingly and for the changes to take effect immediately.

Original Adoption Date (and Board of Governor’s Minutes Item Number): 1998

Revision Date (and Board of Governors’ Minutes Item Number):

Prior Policy Number:

630.0100.98

Schedule for Review:

Divisions/Department Responsible for Review and Update:

Sponsoring Division/Department:

Repeal Date:

Cross Reference:

Procedure(s) for Policy:

Related Policies/References: