

Teaching and Learning Data Domain

Updated: April 2021

Data Domain Scope and Subdomains

The Teaching and Learning data domain comprises four subdomains, whose criteria for inclusion of institutional data are defined as follows:

- **Advising subdomain:** Institutional Data created or stored by UW-Madison students, faculty, staff or contracted service providers as a result of **student academic advising functions** conducted by any means, including (but not limited to) through the use of information technology systems.
- **Assessment subdomain:** Institutional Data created or stored by UW-Madison students, faculty, staff or contracted service providers as a result of individual or aggregate **student, academic program or course assessment functions** conducted by any means, including (but not limited to) through the use of information technology systems.
- **Career Services subdomain:** Institutional Data created or stored by UW-Madison students, faculty, staff or contracted service providers as a result of **career services functions** conducted by any means, including (but not limited to) through the use of information technology systems.
- **Teaching & Learning subdomain:** Institutional Data created or stored as a result of UW-Madison students, faculty, staff or contracted service providers performing **teaching activities or learning activities** by any means, including (but not limited to) through the use of information technology systems.

Relationship to Other Data Domains

All data domains are adjacent to or potentially overlap with other data domains. For Teaching & Learning data attention is primarily given to potential interaction and overlap with the Student Data Domain (trustee: Vice Provost for Enrollment Management). Regular and open communication among the trustees and stewards for these domains is expected.

Data Trustee

Data Trustees are university officials with authority over institutional data, as designated by Data Governance Council. Data trustees are accountable for managing, protecting, and ensuring the integrity and usefulness of institutional data and for upholding UW-Madison policies, UW System policies, state laws, and federal laws applicable to the institutional data.

The Data Trustee for the Teaching and Learning data domain, as assigned by Data Governance Council, is the **Vice Provost for Teaching and Learning**.

Institutional Data Stewards

Institutional data stewards, who are assigned by and accountable to Data Trustees, help define, implement, and enforce data management policies and procedures within their specific data domain.

Institutional Data Domain Profile – Teaching and Learning

Institutional data stewards have delegated responsibility for all aspects of how data is acquired, used, stored and protected throughout its entire lifecycle from acquisition through disposition.

The Institutional Data Stewards for each subdomain of the Teaching and Learning data domain, as assigned by the Data Trustee, are:

- **Advising, Career Services:** Jeff Shokler, Office of Undergraduate Advising
- **Assessment:** Mo Bischoff, Office of the Provost
- **Teaching and Learning:** Dan Voeks, Division of Information Technology

Major Data Systems

UW System Administrative Procedure 1031.A requires Institutional Data Stewards to identify and classify the major systems where data from their data domain resides. System classification level is determined by the highest classification level of data associated with a system but does not indicate that all data associated with the indicated system are necessarily classified at this level. The name and classification of the major systems where Teaching and Learning data reside are:

Major System	Classification	Subdomain
Advising Gateway	Restricted	Advising
Advisor Notes System	Restricted	Advising
AEFIS	Restricted	Assessment; Teaching & Learning
Blackboard Collaborate	Restricted	Teaching & Learning
Canvas	Restricted	Assessment; Teaching & Learning
Engage	Restricted	Teaching & Learning
Handshake	Restricted	Career Services
Honorlock	Restricted	Assessment; Teaching & Learning
Kaltura	Restricted	Teaching & Learning
Piazza	Restricted	Teaching & Learning
Starfish	Restricted	Advising
Tophat	Restricted	Assessment; Teaching & Learning
Turnitin	Restricted	Assessment; Teaching & Learning
Unizin Data Platform	Restricted	Assessment; Teaching & Learning
Zoom	Restricted	Teaching & Learning

Data Classification Rationale

UW System Administrative Policy 1031 and UW-Madison policy UW-504 require that data be classified according to its risk. Within the Teaching and Learning data domain, the classification rationales are:

Advising data subdomain

Classification	Classification Rationale	Example(s)
Restricted	Identifiable Student Record data (including student advising and career services data) are classified as Restricted if data other than FERPA-defined “Directory Information” are exposed.	Course grades, GPA, advisor notes, non-self disclosed career activity, course enrollments, student identification numbers, gender, legal name

Institutional Data Domain Profile – Teaching and Learning

Sensitive	Not applicable to Student Record data (including advising and career services data)	N/A
Internal	Identifiable Student Record (including advising and career services data) data are classified as Internal if the data expose FERPA-defined “Directory Information” only and students with FERPA holds are included in the population. (“FERPA holds” refers to students who have exercised rights under FERPA to opt-out of disclosure for some or all “Directory Information” disclosure).	Directory Information is: preferred name; address (home and mailing); telephone number; email address; major field(s) of study; degree sought; school/college; enrollment status; student type (career); academic level; full-time/part-time status; credit load; credits earned toward degree; expected graduation date/term; intent to participate in commencement; degrees, honors and awards received (type and date); previously attended educational institutions; participation in official athletics; height and weight of athletes
Public	Aggregated Student Record data (including advising and career services data) are classified as Public, unless they are subject to low sample size/population effects where individual students may become identifiable as a result. Identifiable Student Record data are classified as public if the data expose FERPA-defined “Directory Information” only and students with FERPA holds are excluded from the population.	Directory Information is: preferred name; address (home and mailing); telephone number; email address; major field(s) of study; degree sought; school/college; enrollment status; student type (career); academic level; full-time/part-time status; credit load; credits earned toward degree; expected graduation date/term; intent to participate in commencement; degrees, honors and awards received (type and date); previously attended educational institutions; participation in official athletics; height and weight of athletes

Assessment data subdomain

Classification	Classification Rationale	Example(s)
Restricted	Identifiable <i>direct</i> assessment data are protected by FERPA as student records and are classified as Restricted.	Student grades, scores on assignments, and other direct measures of student performance.
Sensitive	Assessment data that are identifiable to students or to instructors are classified as sensitive because the loss of confidentiality and the availability of the data could have a serious adverse impact on individuals.	Survey responses or course evaluations that can be tied to either an identifiable student or an identifiable instructor.
Internal	Assessment data aggregated across students and instructors, but at a lower	Survey or course evaluation summary results for a program or department.

Institutional Data Domain Profile – Teaching and Learning

	level than school or college, are classified as Internal.	
Public	Assessment data aggregated at the institution, school, or college level are classified as Public.	Survey or course evaluation summary results for the institution, a school, or a college.

Career Services data subdomain

Classification	Classification Rationale	Example(s)
Restricted	Identifiable Student Record data (including student advising and career services data) are classified as Restricted if data other than FERPA-defined “Directory Information” are exposed.	Course grades, GPA, advisor notes, non-self disclosed career activity, course enrollments, student identification numbers, gender, legal name
Sensitive	Not applicable to Student Record data (including advising and career services data)	N/A
Internal	Identifiable Student Record (including advising and career services data) data are classified as Internal if the data expose FERPA-defined “Directory Information” only and students with FERPA holds are included in the population. (“FERPA holds” refers to students who have exercised rights under FERPA to opt-out of disclosure for some or all “Directory Information” disclosure).	Directory Information is: preferred name; address (home and mailing); telephone number; email address; major field(s) of study; degree sought; school/college; enrollment status; student type (career); academic level; full-time/part-time status; credit load; credits earned toward degree; expected graduation date/term; intent to participate in commencement; degrees, honors and awards received (type and date); previously attended educational institutions; participation in official athletics; height and weight of athletes
Public	Aggregated Student Record data (including advising and career services data) are classified as Public, unless they are subject to low sample size/population effects where individual students may become identifiable as a result. Identifiable Student Record data are classified as public if the data expose FERPA-defined “Directory Information” only and students with FERPA holds are excluded from the population. (“FERPA holds” refers to students who have exercised rights under FERPA to opt-out of disclosure for some or all “Directory Information” disclosure).	Directory Information is: preferred name; address (home and mailing); telephone number; email address; major field(s) of study; degree sought; school/college; enrollment status; student type (career); academic level; full-time/part-time status; credit load; credits earned toward degree; expected graduation date/term; intent to participate in commencement; degrees, honors and awards received (type and date); previously attended educational institutions; participation in official athletics; height and weight of athletes

Teaching and Learning data subdomain

Classification	Classification Rationale	Example(s)
Restricted	Identifiable student activity data are protected by FERPA as student records and are classified as Restricted.	Access logs, clickstream data or other records characterizing interactive student use of digital learning tools, if these records are personally identifiable and do not consist entirely of Directory Information and do not exclude records of students who have exercised rights under FERPA to opt-out of Directory Information disclosure.
Sensitive	Not applicable	None
Internal	Identifiable student activity data are classified as Internal if the data expose FERPA-defined “Directory Information” only and students with FERPA holds are included in the population. (“FERPA holds” refers to students who have exercised rights under FERPA to opt-out of disclosure for some or all “Directory Information” disclosure).	Access logs, clickstream data or other records characterizing interactive student use of digital learning tools, if these records are personally identifiable and the records consist only of Directory Information and do not exclude records of students who have exercised rights under FERPA to opt-out of Directory Information disclosure.
Public	Student activity data are classified as Public if the data are not identifiable, or if they expose only FERPA-defined “Directory Information” and students with FERPA holds are excluded from the population. (“FERPA holds” refers to students who have exercised rights under FERPA to opt-out of disclosure for some or all “Directory Information” disclosure).	Access logs, clickstream data or other records characterizing interactive student use of digital learning tools, if these records are not personally identifiable or if the records consist only of Directory Information and exclude records of any students who have exercised rights under FERPA to opt-out of Directory Information disclosure.

Additional Information

Data Steward Responsibilities – Teaching and Learning Domain

Responsibilities of Institutional Data Stewards are authoritatively defined by the Institutional Data Policy and by all standards, procedures or other decisions issued by the Data Governance Council.

The following statements express non-binding guidance on behalf of the Teaching and Learning Data Trustee for the use of Teaching and Learning Data Stewards in interpreting and applying the Institutional Data Policy and its accompanying standards in the specific context of the Teaching and Learning Data Domain. In the event of any real or apparent discrepancy between this guidance and the actual authoritative policy and standards, the policy and standards remain fully authoritative.

This guidance shall be updated as needed (e.g. in the event of policy revisions, issuance of new authoritative standards and procedures, substantive changes in guidance from the Data Trustee, or upon the identification of any conflicts between this text and the authoritative policy or standards).

Institutional Data Domain Profile – Teaching and Learning

Institutional Data Stewards assigned to the Teaching and Learning Domain shall:

1. **Ensure Teaching and Learning Data is treated as a shared university resource** and managed for the benefit of the whole university, to support as a first priority the teaching and learning mission of the university and to facilitate campus-wide data-informed decision making.
 - a. *Teaching and Learning Data Stewards shall not prohibit access to Institutional Data except as required by applicable laws, regulations, policies, standards, and procedures, and except where such access is determined (on the basis of the Teaching and Learning Data Trustee’s institutional authority) as inconsistent with the priorities of the University’s teaching and learning mission.*
2. **Responsibly Manage Teaching and Learning Data throughout the entire data lifecycle** in compliance with all applicable laws; Board of Regents, UW System Administration, and university policies, procedures, and standards; and approved records schedules.
 - a. *Teaching and Learning Data Stewards shall ensure institutional data is protected as required by Federal Law (including HIPAA and FERPA), by Wisconsin Statute and/or Administrative code, by any other legal requirements applicable to UW-Madison (including GDPR), by UW System Administrative Policies, and by any applicable UW-Madison policies, including IT, Security and Risk Management policies, and where applicable shall ensure UW-Madison retains ownership rights to institutional data.*
 - b. *Teaching and Learning Data Stewards shall categorize any identified Teaching and Learning Domain Data as subject to applicable UW-Madison records retention schedule(s).¹*
3. **Identify and Document Teaching and Learning Data.** Ensure Teaching and Learning Data sources, elements, processes, integrations, and products are documented and communicated to ensure transparency, clarity, shared understanding, replicability, and ease of use. Promote data literacy through up-to-date and accessible documentation and training resources.
 - a. *Teaching and Learning Data Stewards shall establish, support and oversee a process to ensure existing IT systems storing or processing Teaching and Learning Domain data are inventoried, Data System Custodians identified, characteristics of stored institutional data are recorded, and applicable data classification levels are assigned.*
 - b. *Teaching and Learning Data Stewards shall establish, support and oversee a process to ensure that prior to implementation of any new IT system, any Teaching and Learning Domain data to be stored or processed by the system are inventoried, Data System Custodians identified, characteristics of institutional data are recorded, and applicable data classification levels are assigned.*
4. **Authorize and Manage Access to protected Teaching and Learning data** to protect individual privacy, maintain promised confidentiality, and ensure appropriate access and use. Ensure access to Teaching and Learning data is controlled by reasonable physical, technical, and administrative measures to prevent unauthorized access. Grant access to Teaching and Learning

¹ <https://www.library.wisc.edu/archives/records-management/retention-disposition/>

Institutional Data Domain Profile – Teaching and Learning

data based on appropriateness of an individual's role and the intended use. Document, review, modify, and terminate authorization and access to Teaching and Learning Data in accordance with all applicable laws and UW System university policies, procedures, and standards. Ensure protected Teaching and Learning data is only accessed for business purposes within the scope of an individual's university duties.

- a. When Teaching and Learning Data Stewards receive a request to access Institutional Data or to permit the release of Institutional Data to any party, they shall first determine the applicable Data Classification level(s) and any applicable legal or regulatory requirements.*
 - b. If the requested data are determined to be protected institutional data, Data Stewards shall require that a current risk assessment of physical, technical and administrative controls that would appropriately protect the requested data has been conducted by UW-Madison's Office of Cybersecurity and has been certified by applicable UW-Madison Risk Executive(s). Data Stewards shall examine the risk report and exercise professional judgment to gauge whether any such assessment provides sufficient level of assurance that the examined controls meet the University's data protection obligations, including contractual controls protecting rights of ownership to UW-Madison institutional data where applicable.*
 - c. If applicable controls are determined to be suitable, Data Stewards will exercise professional judgment to make an authorization decision based on criteria including the stated purpose for the requested access and the relationship of the stated purpose to the individual's (or service provider's) role.*
- 5. Share Teaching and Learning Data to the extent allowable under applicable laws, regulations, policies, standards, and procedures.** Ensure Protected Teaching and Learning Data are only made available to those who are explicitly authorized and have an authorized purpose to access it, and individual privacy rights are considered before sharing personally identifiable data.
 - a. Teaching and Learning Data Stewards shall not prohibit access to Institutional Data except as required by applicable laws, regulations, policies, standards, and procedures, and except where such access is determined (on the basis of the Teaching and Learning Data Trustee's institutional authority) as inconsistent with the priorities of the University's teaching and learning mission.*
 - b. Teaching and Learning Data Stewards shall prohibit access to Institutional Data where required by applicable laws, regulations, policies, standards, and procedures.*
- 6. Actively manage the quality and integrity of Teaching and Learning data and data products** and establish explicit criteria for data validity, availability, accessibility, interpretation, and ease of use.
 - a. Teaching and Learning Data Stewards shall establish, support and oversee a process to ensure existing IT systems storing or processing Teaching and Learning Domain data are inventoried, Data System Custodians identified, characteristics of stored institutional data are recorded, and applicable data classification levels are assigned.*

Institutional Data Domain Profile – Teaching and Learning

- b. Teaching and Learning Data Stewards shall establish, support and oversee a process to ensure that prior to implementation of any new IT system, any Teaching and Learning Domain data to be stored or processed by the system are inventoried, Data System Custodians identified, characteristics of institutional data are recorded, and applicable data classification levels are assigned.*
 - c. Teaching and Learning Data Stewards shall establish and oversee a schedule for maintaining and recertifying institutional data inventories as consistent with established Data Quality Standards as required by policy.*
- 7. Classify Teaching and Learning data in accordance with applicable university data classification policy.** Determine and document appropriate classification of Teaching and Learning Data and Data Products. Consider data classification as a factor in Teaching and Learning Data authorization and access procedures.
 - a. Teaching and Learning Data Stewards shall work with Data System Custodians of existing IT systems storing or processing Teaching and Learning Domain data to conduct an inventory to identify and record the characteristics of stored institutional data and assign applicable classification level(s).*
 - b. Teaching and Learning Data Stewards shall work with Data System Custodians of new IT systems prior to implementation to establish an inventory of institutional data to be stored or processed by the system and assign applicable classification level(s).*
 - c. When Teaching and Learning Data Stewards receive a request to access Institutional Data or to permit the release of Institutional Data to any party, they shall first determine the applicable Data Classification level(s) and any applicable legal or regulatory requirements.*
- 8. Ensure any system holding Teaching and Learning data shall be purposefully planned, inventoried, and implemented** to manage Teaching and Learning data throughout the entire data lifecycle in compliance with all applicable laws; Board of Regents, UW System Administration, and university policies, procedures, and standards, including assuring UW-Madison’s rights of ownership to institutional data where applicable; and approved records schedules. Ensure the data lifecycle is integrated into the review and purchase of information technology systems or services and applications that generate, collect, store, maintain, transmit, or record Teaching and Learning data. Ensure systems are documented in a way that enables understanding of the system’s function, the Teaching and Learning data it holds, and how it fits into the university’s overall institutional data architecture and institutional data governance.
 - a. Teaching and Learning Data Stewards shall work with Data System Custodians of new IT systems prior to implementation to establish an inventory of institutional data to be stored or processed by the system and assign applicable classification level(s).*
 - b. Teaching and Learning Data Stewards shall ensure institutional data is protected as required by Federal Law (including HIPAA and FERPA), by Wisconsin Statute and/or Administrative code, by any other legal requirements applicable to UW-Madison*

