

INSTITUTIONAL DATA GOVERNANCE

ADMINISTRATIVE POLICY

This policy pertains to employees.

Policy Statement

Fox Valley Technical College manages institutional data as a strategic asset. Institutional data must be governed, protected, and used responsibly to support decision-making, compliance, and operational effectiveness.

Purpose

This policy establishes requirements for the governance, management, and appropriate use of institutional data to ensure data quality, security, privacy, and accessibility.

Scope

This policy applies to all institutional data and data products, all systems that create or manage institutional data, and all individuals who access, use, or manage institutional data on behalf of the College.

Definitions

Data Domain: a logical grouping of related data assets that share a common business purpose, context, or subject area.

Institutional Data: Data created, collected, managed, or used to support college operations, compliance, and decision-making.

Protected Data: Institutional data that is confidential, sensitive, or subject to legal or regulatory requirements.

System of Record: The official source for a specific data element or dataset.

Roles and Responsibilities

Data Governance Committee: Provides oversight and guidance for institutional data governance; recommends policy, standards, and priorities.

Data Trustees: Accountable for data governance decisions within assigned domains; ensure compliance with applicable laws and College policies; delegate operational responsibilities to Data Stewards as appropriate.

Data Stewards: Implement data governance practices, approve and manage access to institutional data, and oversee data management activities within their assigned domains.

Data System Custodians: Maintain systems that store and process institutional data; implement technical controls to protect institutional data.

Policy Guidelines

Institutional data is a shared college resource and must be managed in a manner that supports the mission and operations of the College.

The College requires the following:

- Institutional data must be governed in accordance with applicable laws, regulations, and college policies.
- Institutional data must be classified according to college standards.
- Access to institutional data must be authorized based on role and legitimate business need.
- Protected data must be safeguarded to ensure confidentiality, integrity, and security.
- Institutional data must be used only for authorized college purposes.
- Institutional data must be sourced from designated systems of record when available.
- Data quality and integrity must be maintained to support accurate and reliable use.
- Institutional data must be shared in a manner that complies with legal, regulatory, and privacy requirements.
- Data governance roles must be defined and maintained to ensure accountability.
- Individuals with responsibilities under this policy must complete required training related to the appropriate use, management, and protection of institutional data, as defined by college standards.
- Exceptions to this policy must be approved and documented in accordance with college procedures.

Compliance

Compliance with this policy is required. Violations may result in loss of access, corrective action, or other disciplinary measures in accordance with College policies and applicable laws.

Related Policies and Standards

- Information Security Policy
- Data Classification Policy
- Acceptable Use of Artificial Intelligence Policy
- FERPA Compliance
- Gramm-Leach-Bliley Act (GLBA)

Adopted: 07/06/2026

Reviewed: 06/08/2026

Revised: N/A