STUDENT DATA PRIVACY

Policy AP 735: Student Data Privacy

This policy applies to all enrolled and prospective students; graduates and their associated data. It applies to all employees who manage and interact with student data at Moraine Park Technical College (MPTC).

This policy is designed to comply with and support federal and state laws related to the handling and privacy of student data including:

- Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Gramm-Leach-Bliley Act (GLBA) Standards for Safeguarding Customer Information (16 CFR Part 314)
- Privacy Act of 1974
- Fair and Accurate Credit Transaction Act of 2003 (FACTA / FTC Red Flags Rule)
- Generally Accepted Privacy Principles as promulgated by the American Institute of Certified Public Accountants (AICPA)

Definitions

- **Education Records**: Records directly related to a student and maintained by the College or a party acting for the College (e.g., grades, transcripts, billing info).
- **Personally Identifiable Information (PII):** Data that can be used to distinguish or trace an individual's identity, including SSN, student ID, or biometric records.
- **School Official:** A person employed by the College in an administrative, supervisory, academic, research, or support staff position; or a contractor/vendor performing an institutional service.
- **Legitimate Educational Interest:** A school official needs to review an education record to fulfill their professional responsibilities for the College.

Processing Related to Legitimate Interest

As an institution of higher education offering undergraduate, adult education, continuing education, non-credit and professional training, Moraine Park requires the collection of personal data to process applications, financial aid, registrations and invoices; and to provide instruction in order to provide students with appropriate industry credentials.

Choice and Consent

By supplying data to Moraine Park Technical College all persons and entities are consenting to the processing of their data for one or more of the specific purposes required for the College's operations. The data subject (person or entity) may revoke the use of data for processing at any time by contacting the College.

Choice, Consent, and Student Rights

By supplying data to Moraine Park Technical College all persons and entities are consenting to the processing of their data for one or more of the specific purposes required for the College's operations. The data subject (person or entity) may revoke the use of data for processing at any time by contacting the College.

In accordance with FERPA, students are granted specific rights regarding their education records:

1. Right to Inspect: Students have the right to inspect and review their education records within 45 days of submitting a written request to the Registrar.
2. Right to Amend: Students have the right to request an amendment to records they believe are inaccurate, misleading, or in violation of their privacy rights.
3. Right to Consent to Disclosure: The College will obtain written consent from a student before disclosing PII from education records, except to the extent that FERPA authorizes disclosure without consent (e.g., to School Officials with a Legitimate Educational Interest).

Note: Consent for internal, mandatory operational data processing required for enrollment, billing, or graduation cannot be fully revoked if a student remains enrolled.

Directory Information & Opt-Out Provision

MPTC designates certain limited student data as "Directory Information," which may be released to third parties without prior written consent (e.g., name, enrollment status, degrees earned). Students have the right to withhold the disclosure of Directory Information by submitting a formal "FERPA Hold" request to the Registrar's Office.

Scope of Data Requested

The policy applies to the following daa collected by the College:

- **Contact Information** including name, email, phone, address.
- **Mobile Number/SMS/Texting:** When users provide their mobile number to the College, they consent to receive informational and transactional SMS messages from the College related to their application, enrollment, account activity, event participation, and other college-related services. Students may opt out at any time. Providing this data is not a condition of enrollment. Standard message and data rates may apply to the use of this technology.
- **Personally identifiable information** including but not limited to birth date, social security number, motor vehicle license, vaccination and health information, education and employment information.
- **Financial Information:** Covered financial data under GLBA, including tuition payment history, bank accounts, financial aid applications (FAFSA data) such as UI//SP-TAX Controlled Unclassified Information/Specified Tax (IRS data provided through the FAFSA application process) and credit information required to establish eligibility for payment or financial aid.
- **Client Reporting data** collected and provided in the aggregate to the Wisconsin Technical College System.

Use, Retention and Disposal

All data processed and stored by the College are to be retained and disposed of in accordance with the College's Records Management Policy and the associated procedures, and federal guidelines, which dictate the maintenance schedules for various operational functions.

Access to subject data is restricted based on employment functions at the College. The access to data is managed by data owners and stewards responsible for various types of data across the College

according to the College's Data Governance Policy and related procedures.

In compliance with the GLBA Safeguards Rule, MPTC actively manages its third-party service providers. The College contractually mandates that all third-party vendors handling student financial and personal data implement, maintain, and certify rigorous administrative, technical, and physical safeguards designed to protect that information.

Disclosure to Third Parties

Moraine Park Technical College will only disclose subject data to governmental and other agencies as prescribed by law, governmental regulations, or authorized statutory exceptions under FERPA. Data subjects are entitled to view records of disclosures released to external entities upon request.

Security and GLBA Safeguards Framework

Data is secured in locked file cabinets (if in paper form) or on secured College servers either on-premises or with an approved third-party vendor. Access to digital or physical data assets is strictly based on the principle of least privilege, mapping an employee's or contractor's access role directly to their operational support requirements.

To meet GLBA Safeguards requirements, the College maintains a comprehensive, written Information Security Program supervised by a designated Program Coordinator. This framework utilizes industry-standard digital security protocols to protect student data, including:

- Regular multi-factor authentication (MFA) requirements for administrative access.
- Annual risk assessments, routine vulnerability tracking, and a formalized Incident Response Plan.

Reason for the Policy

To ensure institutional compliance with applicable federal and state regulations related to student data privacy, security, financial data protection, and identity theft prevention.