STUDENT DATA PRIVACY POLICY

Mandl School, the College of Allied Health, is committed to safeguarding the privacy of student information throughout the academic lifecycle. This policy outlines how student data is collected, used, protected, and shared in accordance with federal and state regulations, including the Family Educational Rights and Privacy Act (FERPA), Title IV of the Higher Education Act, the Gramm-Leach-Bliley Act (GLBA), and requirements set by the New York State Education Department (NYSED).

Definition of Student Data

"Student data" refers to any information that identifies or could reasonably identify a student, including:

- Academic records
- Financial aid details
- Contact and demographic information
- Credentials used in online platforms
- Personally identifiable information (PII)

Mandl collects only the data necessary to support academic, administrative, and compliance functions.

Protection of Student Data

Use of Secure Technology Platforms

Mandl uses secure, compliant platforms such as Microsoft Teams and Canvas for online instruction. These platforms are configured to meet or exceed FERPA, Title IV, NYSED, and GLBA standards.

Key protections include:

- All digital communications use TLS/HTTPS encryption.
- Student data is encrypted both in transit and at rest.
- Students must create a personalized password upon first login and activate Multi-Factor Authentication (MFA) via the Microsoft Authenticator app.
- All technology partners are regularly reviewed to ensure data privacy compliance.

Access Controls

Access to student data is restricted to authorized personnel with a legitimate educational or operational need. Access levels are governed by role-based permissions and reviewed regularly by Mandl's Online IT Coordinator.

Data Retention and Deletion

Mandl retains student records in accordance with federal and state laws, including a minimum three-year retention period for Title IV records after a student's last year of attendance (34 CFR 668.24). Once records reach the end of their retention period, they are securely deleted or anonymized.

Disclosure of Privacy Practices and Student Rights
Students are informed—prior to enrollment—about how their data will be collected, used, stored, and protected. This information is available in the institutional catalog and on the Mandl website under the Consumer Information tab.

As part of Mandl's transparency and compliance with ABHES Standard V.H.3, students are also notified in writing of any potential impediments to program completion or future employment (e.g., criminal background, licensure requirements).

Training, Oversight, and Compliance
All employees, faculty, and contractors who handle student information must complete ongoing data privacy and security training. Mandl affirms institutional compliance through its Program Participation Agreement (PPA) and routinely audits data practices to remain aligned with FERPA, Title IV, GLBA, NYSED, and accreditation standards.

Incident Response and Data Breaches
In the event of a suspected or confirmed data breach, Mandl will activate its Incident Response Plan, which includes:

- Prompt notification of affected students and appropriate authorities
- Mitigation efforts to reduce potential harm
- Remedial actions to improve systems and prevent recurrence

Cybersecurity and Identity Protection Compliance
Mandl complies with the GLBA Safeguards Rule, maintaining a written Information Security Program that includes regular risk assessments, ongoing monitoring, technical safeguards, and identity theft prevention measures. This program is updated regularly to reflect evolving federal and state cybersecurity guidance.

Departmental Responsibilities:

- IT Department: Maintains secure systems, manages access controls, monitors for threats, and supports incident response efforts in alignment with federal data protection standards.
- Registrar and Administrative Offices: Ensure the accuracy and proper retention or disposal of student records.
- All Employees and Contractors: Must adhere to privacy protocols, complete assigned training, and report any suspected violations.

Policy Review
This policy is reviewed and updated annually, or as needed to reflect changes in laws, regulations, or institutional procedures. Revisions are overseen by a designated committee.