Protecting Student Information

Published 1/11/2022 by Cheryl Kennedy

Seneca recognizes that students value their privacy and want to be assured that their personal data is protected and used for authorized purposes. Seneca takes this role seriously and has taken steps to ensure that there are measures in place to secure the information collected from students, and to protect it from unauthorized use, disclosure or loss. The following are just some of the examples of the safeguards in place at Seneca:

Administrative Safeguards:

- Privacy and Security policies and procedures
- Employee privacy and security training
- Confidentiality Agreements and clauses
- Privacy Impact Assessments

Technical Safeguards:

- Role-based access controls
- Multifactor Authentication
- Strong passwords and encryption
- Maintaining up-to-date software and applying patches
- Firewalls, intrusion detection and prevention, anti-virus and anti-spam solutions
- Centralized logging for auditing and forensic purposes
- Robust data backup schedule
- Periodic validation of implemented security controls by independent third parties

Physical Safeguards:

- Controlled access to locations where personal information is stored
- Locked cabinets
- Access cards and keys

Seneca has a dedicated Privacy Office and ITS Security and Compliance team that remains

up-to-date on industry standards, identifies and responds to trends such as developing specialized resources for areas that handle sensitive information, and recommends additional privacy protective measures as required. To learn more about our team, visit the IT Security or Privacy Office intranet pages.

tags : data-privacy, data-privacy-month, safeguards, security-controls, student-news, student-privacy