



POLICIES and PROCEDURES

Responsible Unit	Chief Privacy Officer
Last Reviewed/Updated	1 December 2020
Approving Sector Head	President and Vice-Chancellor
Policy	Acadia University Information Privacy and Data Security

Purpose and Intent

To ensure Acadia University complies with its obligation to protect personal and private information under *Nova Scotia's Freedom of Information and Protection of Privacy Act* and *Personal Information International Disclosure Act* which governs the storage and access to information outside of Canada and the Canadian *Personal Information Protection and Electronic Documents Act*, as well as the *General Data Protection Plan*.

To ensure Acadia has a process in place to inform its employees about their personal obligations with respect to handling, storing and reporting of information and that employees agree to abide by this policy.

Definitions

"Personal information" means recorded information about an identifiable individual, including, but not limited to: a. name, address, telephone, email (personal not business); b. race, ethnic origin or religious political beliefs or associations; c. age, sex, sexual orientation, marital status or family status; d. any identifying number or symbol (examples: ID Card, SIN, credit card, health insurance, drivers' license); e. fingerprints, blood type, or inheritable characteristics; f. medical or personal history; g. educational, employment, financial, or criminal history; h. personal views or opinions.

Policy Statement

Acadia employees will protect the privacy and data security of personal and confidential information of employees, students (prospective and current), alumni, suppliers, contractors, data collected during research, and all other information collected during the course of Acadia's ongoing operation and activities and agree to report any privacy, confidentiality or security breaches, immediately upon discovery.

Jurisdiction

The **Acadia University Information Privacy and Data Security Policy** applies to all members of the Acadia University community: faculty, staff, students, contracted employees working on university property or remotely on behalf of the university, and visitors and guests of Acadia University or of members of the University community.

Disclosure, Reporting and Response

Acadia is bound by Federal and Provincial legislation to report privacy and security breaches, to respond to request for disclosure of information, and to complete reports requested by government agencies with respect to Acadia's business practices. Acadia and its agents will comply with these obligations and the timelines provided within these various *Acts*.

Employee Compliance

Employees have a duty to familiarize themselves with this policy, all applicable government *Acts* and *Regulations*, and to complete the security awareness training provided by the University.

Employees' supervisors have an obligation to ensure the information and data risks in their department are fully understood by all direct reports and that adequate and appropriate security measures are in place.

Employees have a duty to report any privacy, confidentiality or security breaches, immediately upon discovery, to persons within Acadia responsible for securing and/or reporting the breach.

Related Resources

[Acadia's Privacy and Data Security website](#)

[Acadia's Academic Calendar \(Registrar\)](#)

[Acadia's Security Awareness Training \(Technology Services\)](#)

[Report a CyberSecurity or Privacy Event \(Technology Services HUB\)](#)

[NS Freedom of Information and Protection of Privacy Act](#)

[NS Personal Information International Disclosure Act](#)

[Personal Information Protection and Electronic Documents Act \(Canada\)](#)

[General Data Protection Regulation \(GDPR\) Compliance Guidelines](#)