COMMISSION SCOLAIRE SIR-WILFRID-LAURIER
SIR WILFRID LAURIER SCHOOL BOARD

Policy no. 2023-CA-28	**Information Security**

Approved:	**Resolution no.**	**CC-240424-CA-0092**
Revised:	**Resolution no.**	
~~**Origin:**~~	~~**Secretary General**~~	

NOTE: In keeping with its commitment to respecting diversity, the Sir Wilfrid Laurier School Board uses gender-inclusive language in all its written communications. In cases where eliminating references to gender is not possible, gender-specific pronouns and possessive determiners are used solely for purposes of clarity and concision.

1.0 CONTEXT

In the course of its activities, the Sir-Wilfrid-Laurier School Board (hereinafter "SWLSB") processes a significant amount of data in multiple formats. Given the nature of this data, SWLSB must ensure its appropriate handling. The SWLSB must put in place a series of measures to ensure proper and flexible management of the information held, in order to comply with various legal and regulatory obligations. In this regard the *Act respecting the governance and management of the information resources of public bodies and government enterprises* (AGMIR, LRQ, and Bill 133) and the *Directive sur la sécurité de l'information gouvernementale* (DSIG, a directive of the Secrétariat du Conseil du trésor du Québec applicable to school boards and school service centres) impose obligations on educational institutions in their capacity as public bodies. Notably, they require that school boards and school service centres adopt, implement, update and enforce an *Information Security Policy* (hereinafter "Policy") in order to ensure confidentiality, integrity and availability of the information it stores, transfers, and uses in the course of its activities.

2.0 OBJECTIVES

This Policy aims at promoting best practices and raising awareness among the SWLSB stakeholders in order to comply with legal requirements and reduce risks while protecting the information it stores, transfers, and uses. The SWLSB wishes to reaffirm its commitment and ongoing efforts in order to ensure the confidentiality, integrity and availability of information. In this regard, this Policy complements the SWLSB's *Use of Information and Communication Technology Resources Policy* which notably stated its commitment to provide and maintain a secure, effective and reliable information technology infrastructure.

3.0 FRAME OF REFERENCE

- The *Charter of Human Rights and Freedoms* (LRQ, c. C-12)
- The *Education Act* (LRQ, c. I-13.3)
- The *Regulation respecting retention schedules, transfer, deposit and disposal of public archives* (LRQ, c. A-21.1, r.1)
- The *Civil Code of Quebec* (LQ, 1991, c. 64
- The *Policy Framework for the Governance and Management of the Information Resources of Public Bodies*

- The *Act respecting the governance and management of the information resources of public bodies and government enterprises* (LRQ, Bill 133)
- The *Act to establish a legal framework for information technology* (LRQ, c. C-1.1)
- The *Act respecting access to documents held by public bodies and the protection of personal information* (LRQ, c. A-2.1)
- The *Criminal Code* (R.S.C., 1985, c. C-46)
- The *Regulation respecting the distribution of information and the protection of personal information* (c. A-2.1, r. 2)
- The *Directive sur la sécurité de l'information gouvernementale*
- The *Copyright Act* (R.S.C., 1985, c. C-42)
- The SWLSB Policy No. 2000-IT-01 - *Use of Information and Communication Technology Resources Policy*
- SWLSB Policy no. 2018-CA-23 - *Policy Governing the of Disclosure of Wrongdoings*
- SWLSB Policy no. 2011-HR-08 - *Code of Conduct for all Employees of the Sir Wilfrid Laurier School Board*
- SWLSB By-Law no. BL2009-CA-17- *Code of Ethics & Professional Conduct for Commissioners of the Sir Wilfrid Laurier School Board*
- SWLSB Policy no. 2005-CA-12- *Communication Policy*

4.0 SCOPE

This Policy applies at all times to all SWLSB information users – employees, youth and the adult and vocational sector students, commissioners, consultants, parents, partners, volunteers, suppliers and vendors – who access and/or use SWLSB information assets, regardless of the storage format, the means used to create, access and/or communicate the information, the location from which the information is accessed, saved and/or transmitted, and whether or not the information is managed or owned by the SWLSB or a third party.

5.0 GUIDING PRINCIPLES

The following guiding principles govern the SWLSB's action pertaining to information security:

5.1 Develop a full understanding of the information that needs to be protected;

5.2 Recognize the importance of this Policy;

5.3 Understand that the technological environment for digital and non-digital information assets changes constantly;

5.4 Protect information throughout its life cycle (creation, processing, destruction);

5.5 Ensure that employees have access only to information that is required to perform their normal duties;

5.6 The use of digital and non-digital information assets must be governed by a policy or directive that explains the appropriate procedure to follow and sets out what is permitted and what is not.

6.0 AWARENESS AND TRAINING

Information security depends largely on regulating personal conduct and ensuring individual accountability. For this reason, the members of the SWLSB community must be trained and/or made aware of:

- Information security and the SWLSB's information systems;
- Security directives;
- Risk management;
- Incident management;
- Existing threats;
- The consequences of a security breach;
- Their role and responsibility in matters of security.

7.0 COMMITTEES

7.1 The Committee on Information Security and the Access and Protection of Personal Information

Among the obligations under the *Act respecting access to documents held by public bodies and the protection of personal information*, the Committee on Information Security and the Access and Protection of Personal Information (the Committee) will also be responsible for carrying out its responsibilities related to the protection and access of personal information. It will also be responsible for the implementation of this Policy and will create the Management Framework which will outline the Committee's responsibilities.

The Committee is composed of representatives from Legal Corporate and Communications, Human Resources and Information Resources as named by the Director General. Other representatives can be invited, if relevant.

~~The Committee is composed of:~~

- ~~Director - Legal, Corporate and Communications Department;~~
- ~~Assistant Director - Legal, Corporate and Communications Department;~~
- ~~Director - Information Resources;~~
- ~~Coordinator - Information Resources;~~
- ~~Superintendant - Information Resources;~~
- ~~Coordinator - Human Resources;~~
- ~~Librarian - Legal, Corporate and Communications Department;~~
- ~~Representatives of other departments can be invited when deemed relevant.~~

7.2 Crisis Management Team

A Crisis Management Team is created to ensure a proper response to major incidents and ensure the continuity of the SWLSB's operation in such instances. The Crisis Management Team will collaborate with the Committee on Information Security and the Access and Protection of Personal Information when required.

The Information Security Crisis Management Team is composed of:

- The Director General or a representative;
- The Organizational Information Security Coordinators (coordonnatrices organisationnelles ou coordonnateurs organisationnels des mesures de sécurité de l'information);
- The Person Responsible for Information Security;
- A representative of the communications team;
- Any other member of the management team whose department/school/centre is impacted by the information security incident.

8.0 SANCTIONS

Any SWLSB employee who contravenes the legal framework, this Policy or the information security measures resulting from it, is subject to sanctions in accordance with the nature, severity and consequences of the contravention, as prescribed by applicable law or internal disciplinary regulations (including those stipulated in the collective agreements, the SWLSB policies and by-laws, and the code of conduct for employees). Students, suppliers, partners, guests, consultants and external organizations are subject to the sanctions deemed appropriate by the SWLSB.

9.0 DISTRIBUTION AND UPDATES

This Policy shall be reviewed periodically in order to evaluate its efficiency and updated accordingly.

10.0 MANAGEMENT FRAMEWORK

A Management Framework will be established by the Committee on Information Security and the Access and Protection of Personal Information in order to define the SWLSB's stakeholders' roles and responsibilities with respect to this policy and in order to list measures that will promote the security, integrity and confidentiality of information. This Management Framework will be updated on a regular basis by the Committee considering the evolving nature of the digital environment.

11.0 EFFECTIVE DATE

This policy will come into force on the date of its adoption by the Council of Commissioners.

v. 2023-06-09