

Policy Statement



Policy No. E-11

SUBJECT: Information Security Policy

Approval Date: March 26, 2019

Resolution No: C-18/19-165

Revision Date:

Resolution No:

Revision Date:

Resolution No:

Origin: Council of Commissioners

1. CONTEXT

The *Act respecting the governance and management of the information resources of public bodies and government enterprises* (RLRQ, c.g-1.03) and the *Directive sur la sécurité de l'information gouvernementale* (DSIG, a directive of the Québec Treasury Board applicable to school boards) impose obligations on educational institutions in their capacity as public bodies.

The *Directive sur la sécurité de l'information gouvernementale* requires that school boards adopt, implement, update and enforce an information security policy—whose main provisions are set out in the government's directive—specifically through formal information security processes that make it possible to manage risks, access to information and incidents.

This policy enables the Western Quebec School Board to achieve its missions, maintain its reputation, comply with legal requirements, and reduce risks while protecting the information it creates or receives.

This information pertaining to human, physical, technological and financial resources is accessible in digital and non-digital formats; risks threatening the accessibility, integrity and privacy of that information can have consequences that compromise:

- The life, health or wellbeing of individuals
- The protection of personal information and privacy
- The delivery of services to the public
- The image of the school board and of the government.

2. OBJECTIVES

The goal of this policy is to affirm the school board's commitment to fully discharge its obligations pertaining to the security of information, wherever it is stored and however it is communicated. More specifically, the school board is responsible for:

- The availability of information when and how authorized persons require it;

- The integrity of information such that it is neither destroyed nor altered in any way without authorization and that the medium used to store it provides the desired stability and sustainability;
- The privacy of information by limiting its disclosure and use to authorized persons, especially when it contains personal information.

The school board has therefore adopted this policy in order to orient and define its vision, which is detailed in the school board's management framework for information security.

3. LEGAL AND ADMINISTRATIVE FRAMEWORK

This security policy is governed primarily by the following:

- The *Charter of human rights and freedoms* (RLRQ, c. C-12)
- The *Education Act* (RLRQ, c. I-13.3)
- *Regulation respecting retention schedules, transfer, deposit and disposal of public archives* (RLRQ, c. A-21.1, r.1)
- The *Civil Code of Québec*
- 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 (RLRQ, c.g-1.03)
- The Act to establish a legal framework for information technology (RLRQ, c. C-1.1)
- The Act respecting access to documents held by public bodies and the protection of personal information (RLRQ, 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* (RLRQ, 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)

Local Documents in reference to the present policy:

- *The Policy of Appropriate Use of Information & Communication (No. E-9)*
- *The policy of Code of Conduct for employees and volunteers of the WQSB (No. F-17)*
- *The Policy of Video Surveillance (No. E-10)*
- *The Information Security Management Framework*

4. SCOPE OF APPLICATION

This policy is intended for information users, i.e. all staff and any natural or legal person who, as an employee, consultant, partner, supplier, student or member of the public, uses the school board's information assets. All users have an obligation to protect information assets made available to them by the school board. To this end, users must:

- Be aware of this policy, as well as of any directives, procedures and other guidelines arising therefrom;
- Use the information assets made available to them solely for the intended purposes, and this in accordance with assigned access rights and only when necessary to the performance of their duties;
- Respect the security measures installed on their work station, and on any other equipment containing information that needs to be protected, and never modify their configuration or deactivate them;
- Comply with legal requirements governing the use of products for which intellectual property rights may exist;

- e. Immediately report to their superior any act of which they become aware that may constitute a real or presumed violation of security regulations, as well as any problem that might threaten the security of the school board's information assets.

This refers to all information, digital and non-digital, that the school board holds in the context of its activities, whether storage of that information is managed by the school board or by a third party.

5. **GUIDING PRINCIPLES**

The following guiding principles inform the school board's actions pertaining to information security:

- a. Develop a full understanding of the information that needs to be protected, including a clear identification of holders and their security profile;
- b. Recognize the importance of the information security policy;
- c. Understand that the technological environment for digital and non-digital information assets changes constantly and is interconnected with the world;
- d. Protect information throughout its life cycle (creation, processing, destruction);
- e. Ensure that employees have access only to information that is required to perform their normal duties;
- f. 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. **SANCTIONS**

Any school board 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 collective agreements and the school board by-laws).

Suppliers, partners, guests, consultants and external organizations are subject to these sanctions.

7. **DISTRIBUTION AND UPDATES**

With the assistance of the General Director, the RSI is responsible for distributing and updating the management framework. The management framework shall be reviewed periodically in accordance with updates made to it.

8. **EFFECTIVE DATE**

This framework came into effect on the date of the adoption by the council of commissioner.