Adopted: 2019-12-03
Revised: 2023-06-27

POLICY EF

INFORMATION SECURITY

This policy affirms the New Frontiers School Board's (NFSB) commitment to fully discharge its obligations pertaining to the security of information, wherever it is stored and however it is communicated. More specifically, NFSB is responsible for:

- The availability of information so that it is accessible in a timely manner to authorized person(s);
- 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.

Note: Where the word "unit" appears, it may apply to any administrative units, such as schools, centres, and departments. Where the term "Director" or "Director of" is used, it is taken to mean "a" or "the" administrator responsible for the department or function.

CONTEXT

The *Act respecting the governance and management of the information resources of public bodies and government enterprises* (AGMIR, LRQ, Bill 133) and the *Directive sur la sécurité de l'information gouvernementale* (DSIG, directive of the Québec Treasury Board to school boards) imposed obligations on educational institutions in their capacity as public bodies. As stipulated in the *Appointment Guide*, every school board is required to have an information security manager (RSI) and two (2) sector coordinators for incident management (CSGI).

This policy enables NFSB to maintain its reputation, comply with legal requirements, and reduce risks while protecting the information it creates or receives, and for which it is responsible. 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 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.

SCOPE

This policy is intended for "information users", such as staff and any natural or legal person who, as an employee, consultant, partner, supplier, student, volunteer, 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:

a) Be aware of and adhere to this policy, as well as any directives, procedures, and other guidelines arising therefrom, and comply with provisions therein;
b) 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;
c) Respect the security measures installed on their workstation, and on any other equipment containing information that needs to be protected, and never modify their configuration or deactivate them;
d) Comply with legal requirements governing the use of products for which intellectual property rights may exist;
e) Report and record, using the appropriate form, with their immediate supervisor 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, non-digital, verbal) that information users hold in the context of their activities, whether storage of that information is managed by the School Board or by a third party.

GUIDING PRINCIPLES

The following guiding principles inform the NFSB'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) Understand that the technological environment for digital and non-digital information assets changes constantly and is interconnected with the world;
c) Protect information throughout its life cycle (creation, processing, destruction);
d) Ensure that employees have access only to information that is required to perform their normal duties;
e) Ensure users are informed as to the appropriate utilization of digital and non-digital information assets.
f) Ensure users do not share confidential information, or their access to it, unless specific authorization has been granted.

SANCTIONS

Any information user who contravenes 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 school board policies). Any resulting penalty or fine may be transferred to the information user.

LEGAL & ADMINISTRATIVE FRAMEWORK

This security policy is governed primarily by or related to:

- The *Charter of human rights and freedoms* (LRQ, c. C-12)
- The *Education Act* (LRQ, c. I-13.3)
- *Regulation respecting retention schedules, transfer, deposit and disposal of public archives* (LRQ, c. A-21.1, r.1)
- The *Civil Code of Québec* (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 information resources of public bodies and government enterprises* (RSQ, Bill 133);
- Law 25 (Bill 64) *An Act to Modernize Legislation Provisions Respecting the Protection of Personal Information;*
- 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* (RSQ, chapter A-2.1);
- The *Criminal Code* (RSC, 1985, chapter C-46);
- The *Regulation respecting the distribution of information and the protection of personal information* (chapter A-2.1, r.2);
- The *Directive sur la sécurité de l'information gouvernementale*;
- The *Copyright Act* (RSC, 1985, chapter C-42);
- All related NFSB policies, organizational guides, or procedures

End.