WESTERN QUEBEC SCHOOL BOARD
DIRECTIVE RESPECTING ROLES AND RESPONSIBILITIES IN THE EVENT OF A CONFIDENTIALITY INCIDENT

1. LEGAL FRAMEWORK

The present directive stems from sections 63.8 to 63.11 of the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (CRLQ, c.A-2.1), hereinafter "the Act".
This directive is to be read in conjunction with other tools available at the Western Quebec School Board (hereinafter "WQSB").

2. PURPOSE AND OBJECTIVES

The purpose of this directive is to ensure the implementation of the obligations of the WQSB under the Act in relation to confidentiality incidents.
The objectives of this directive are as follows:

- State the principles underlying the protection of personal information collected, used, released, and retained in the course of performing the functions of the WQSB.
- Establish a process for reporting confidentiality incidents that may occur in the course of WQSB functions.
- Inform staff and others in the WQSB about confidentiality incidents.
- Identify the roles and responsibilities of persons covered by this directive.

3. SCOPE

This directive applies to all WQSB personnel in all schools, centres and departments. It also applies to the members of the Council of Commissioners, Executive Committee, Education Committees (including the parents and volunteers serving on these committees).
This directive does not limit the WQSB's responsibilities under its information security policy adopted pursuant to the Act Respective the Governance and Management of the Information Resources of Public Bodies and Government Enterprises (R.S.Q., c. G-1.03) and the regulations and directives issued thereunder.

4. DEFINITIONS

The terms used in this directive are those of the Act and other applicable legal frameworks, unless otherwise specified.
To facilitate the understanding of this directive, the following definitions apply:

Committee
WQSB's Committee on Access to Information and the Protection of Personal Information

Confidentiality Incident

1. Access not authorized by law to personal information.
2. Use not authorized by law of personal information.
3. Release not authorized by law of personal information.
4. Loss of personal information.
5. Any other breach of the protection of such information.

Declarant
A person who has knowledge of a possible confidentiality incident.

Designated Person Responsible for the Protection of Personal Information
Person designated by Council (hereinafter "Designated Person") under the Act who is responsible for coordinating and oversight of the protection of personal information within the WQSB.

Person
A person covered by the scope of this directive acting on behalf of the WQSB.

Personal Information
Information concerning a natural person that allows the person to be identified directly or indirectly.

5. GENERAL PRINCIPLES

5.1. A Person shall only collect personal information that is necessary for the functions of the WQSB.

5.2. A Person shall have access only to personal information that is necessary for the performance of their duties.

5.3. A Person shall not release personal information without the consent of the individual, their representative or as required by law.

5.4. A Person who becomes aware of a confidentiality incident must promptly report it in accordance with this directive.

6. PROCEDURE DURING A CONFIDENTIALITY INCIDENT

6.1. Reporting of a confidentiality incident

6.1.1. The Declarant must, without delay, inform their immediate supervisor of any event that could lead to the belief that a confidentiality incident has occurred.

6.1.2. As much as possible, the Declarant shall provide the following information with respect to the confidentiality incident:

- The context and circumstance surround the event (date, description of what happened, etc.).
- The nature of the personal information involved (name, address, email, permanent code, etc.).
- Whether or not the information was password/passcode protected.
- The number of individuals to whom the personal information relates.
- The identity and number of individuals or organizations that received the information, if applicable.
- The measures taken, if applicable.
- Any other relevant information.

6.1.3. The Declarant and supervisor must, as soon as possible, take the necessary actions that would reduce the risk of harm being caused (for example, recalling an email, telephone communications, etc.)

6.1.4. The supervisor shall promptly inform the Designated Person of the event reported and provide them will all relevant information.

6.2. Analysis of the Situation Reported

6.2.1. The Designated Person analyses the situation reported, and, if necessary, obtains additional information.

6.2.2. The Designated Person determines whether the situation is a confidentiality incident.

6.2.3. If it is determined that the situation does not constitute a confidentiality incident, but that an intervention is still necessary with the persons involved, the Designated Person communicates with the management/supervisor so that they can take the appropriate action, if necessary.

6.3. Handling of a Confidentiality Incident

6.3.1. The Designated Person shall ensure that all actions or measures, including those taken by the Declarant or supervisor, which are likely to reduce the risk of injury to individuals whose personal information is affected by the confidentiality incident, are implemented. For example:

- Obtain from individuals to whom personal information has been unlawfully released, confirmation of the destruction of the personal information obtained.
- Obtain from individuals to whom personal information has been unlawfully released an undertaking of non-disclosure of the personal information obtained.
- Recommend intervention with affected employees.

6.3.2. The Designated Person shall assess the risk of serious injury from the confidentiality incident by considering, among other things, the sensitivity of the information, the perceived consequences of its use, and the likelihood that it will be used for harmful purposes. If the confidentiality incident is determined to present a serious risk, the Designated Person shall:

- Notify the Commission d'accès à l'information diligently, in the manner and with the information required by the applicable regulation.
- Notify any individual whose personal informal is affected by the confidentiality incident in the manner and by providing the information required by the applicable regulation.
- Notify any person or agency that may reduce the risk of serious harm (the Ministry, police, etc.) by releasing only the personal information necessary for this purpose and record this release in the Act register.

6.3.3. The Designated Person shall record the incident in the confidentiality register in all cases.

6.4. Measures to be Taken to Prevent a Similar Confidentiality Incident from Occurring Again

6.4.1. Once the immediate measures have been completed, the Designated Person determines whether other measures should be implemented to prevent the recurrence of similar incidents. For example:

- Modification of digital access.

- Deleting personal information.
- Implementation of training or other awareness measures.
- Reviewing internal processes (software, work methods, etc.)

7. COMMITTEE

7.1. The Designated Person may, at any time, consult the Committee in the analysis and treatment of a situation that may be a confidentiality incident.

7.2. The Designated Person shall report annually to the Committee on Access on confidentiality incidents that have occurred and the measures implemented.

7.2.1. In all cases, the Designated Person shall forward to the Committee the recommendations of the Commission d'accès à l'information, if any.

8. INFORMATION AND PROMOTION

The Designated Person shall ensure that this directive is distributed to the various administrative units, and, when necessary and in collaboration with school administrators, ensure that adequate training is available and offered to staff.

9. COMING INTO FORCE

This directive comes into force July 15, 2026.