



Commission scolaire English-Montréal
English Montreal School Board

DIRECTIVE SG 3-24

DIRECTIVE RESPECTING ROLES AND RESPONSIBILITIES IN THE EVENT OF A CONFIDENTIALITY INCIDENT

Coming into force on February 6, 2024

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 “ARA”).

This directive must be read in conjunction with the various tools available at the English Montreal School Board, hereinafter “EMSB”, concerning the protection of personal information.

2. PURPOSE AND OBJECTIVES

The purpose of this directive is to ensure the implementation of the EMSB’s obligations under the ARA in relation to confidentiality incidents.

The objectives of the 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 EMSB;
- Establish a process for reporting confidentiality incidents that may occur in the course of the functions of the EMSB;
- Inform staff and others at the EMSB about confidentiality incidents;
- Identify the roles and responsibilities of persons covered by this policy.

3. FIELD OF APPLICATION

This directive applies to all EMSB personnel (schools, centers, departments). It also applies to the members of the Council of Commissioners, the members of the governing boards and the members of the various committees of the EMSB.

This directive does not limit the EMSB’s responsibilities under its Information Security Policy adopted pursuant to the *Act respecting 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 ARA and other applicable legal frameworks, unless otherwise indicated.

To facilitate the understanding of this directive, the following definitions apply:

Committee on Access	Access to information and privacy committee of the EMSB.
Declarant	Person having knowledge of a possible confidentiality incident.
Confidentiality incident	<ol style="list-style-type: none">1. Access not authorized by law to personal information.2. Use not authorized by law to 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.
Person	Person covered by the scope of this directive acting on behalf of EMSB or in the course of their duties.
Personal information	Information concerning a natural person which allows the person to be, directly or indirectly, identified.
Person in Charge	Person designated as the Person in charge of the protection of personal information within the EMSB.

5. GENERAL PRINCIPLES

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

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 shall 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 the management of their administrative unit (school, center, department) of any event that could lead to the belief that a confidentiality incident has occurred.

6.1.2. To the extent possible, the Declarant shall provide the following information with respect to the confidentiality incident:

- The context and circumstances surrounding the event (date, description of what happened, etc.);
- The nature of the personal information involved (e.g., name, address, email, permanent code, etc.);
- Whether or not the information was protected by a password or access code, for example;
- 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 management must, as soon as possible, take the necessary actions that would reduce the risk of harm being caused (recalling of an email; telephone, etc.).

6.1.4. Management shall promptly inform the Person in Charge of the event that has been reported to it and provide them with all relevant information.

6.2. Analysis of the situation reported

6.2.1. The Person in Charge analyses the situation reported.

6.2.2. If necessary, they obtain additional information.

6.2.3. They decide on the situation and determine if it is a confidentiality incident.

6.2.4. If they determined that the situation does not constitute a confidentiality incident, but that an intervention is still necessary with the persons involved, they communicate with management so that they can take the appropriate action, if necessary.

6.3. Handling of a confidentiality incident

6.3.1. The Person in Charge shall ensure that actions or measures, which are likely to reduce the risk of injury to individuals whose personal information is affected by the confidentiality incident, are implemented considering those taken by the Declarant or management, as appropriate.

6.3.2. The Person in Charge 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.

6.3.3. If the confidentiality incident presents a serious risk, the Person in Charge 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 information is affected by the confidentiality incident in the manner and by providing the information required by the applicable regulation;
- No notice to affected persons is required if the effect of such notice would be to impede an investigation by a person or agency that is charged by law with preventing, detecting or suppressing crime or violations of law;
- Notify any person or agency that may reduce the risk of serious harm (ministry, police, etc.) by releasing only the personal information necessary for this purpose and record this release in the ARA register.

6.3.4. The Person in Charge 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 Person in Charge determines whether other measures should be implemented to prevent the recurrence of similar incidents.

7. COMMITTEE ON ACCESS

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

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

7.3. In all cases, they shall forward to the Committee on Access the recommendations of the Commission d'accès à l'information, if any.

8. INFORMATION AND PROMOTION

- 8.1. The Person in Charge shall ensure that this directive is distributed to the various administrative units.
- 8.2. When necessary, in collaboration with school administrations, the Person in Charge ensures that adequate training is available and offered to staff members.

9. COMING INTO FORCE

This directive comes into force on February 6, 2024.