# INFORMATION SECURITY

## Background

The Board is committed to managing records, data, and information as an indispensable and strategic resource. The Board believes that the Division's approach to information security should be consistent with provincial standards and should enable business and educational outcomes.

The Board ensures that the Division fulfills its dual legislative obligations to maintain public accountability and openness through the Access to Information Act (ATIA) while providing robust protection of personal privacy under the Protection of Privacy Act (POPA).

## Guiding Principles

All records and information collected and created in the service of the Division remain the property of the Division, which is accountable for managing these records throughout their entire life cycle.

1. **Accountability**
   The responsibilities and accountability of the Division, its staff and all users of Division information systems should be explicit.

2. **Awareness**
   The Division, its staff and all users of Division information should be aware of the need for the security of information systems and what they can do to enhance security.

3. **Ethics**
   The information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.

4. **Multidisciplinary**
   Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints.

5. **Proportionality**
   Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm.

6. **Integration**

Measures, practices and procedures for the security of information systems should be coordinated and integrated with other measures, practices and procedures of the organization so as to create a coherent system of security.

7. **Timeliness**
   The Division should act in a timely, coordinated manner to prevent and respond to breaches of security of information systems.

8. **Reassessment**
   The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. **Transparency**
   The security of information systems should be compatible with the legitimate use and flow of data and information in an open and accountable public institution.

**Board Responsibilities**

**The Board shall:**

**1.** Exercise governance authority in accordance with Board Policy 11 - Delegation of Authority, including the appointment of the Privacy Officer to ensure compliance with privacy legislation.

**2.** Trustees shall have access to the information reasonably required to fulfill their responsibilities as members of the Board, subject to applicable legislation, confidentiality requirements, Board policy, and established processes.

**3.** Receive notice of any significant breaches of information security in a timely manner.

Legal Reference: Section 52, 53, 65, 68, 222 Education Act
Access to Information Act (ATIA)
Protection of Privacy Act (POPA)
Protection of Privacy (Ministerial) Regulation 143/2025
Administrative Procedure 180 - Access to Information and Protection of Privacy
Administrative Procedure 185 - Records Management