EDMONTON PUBLIC SCHOOLS

Board Policy

CODE: CNA.BP

TOPIC: Information Security

EFFECTIVE DATE: (28-01-2020)

ISSUE DATE: (29-01-2020)

REVIEW YEAR: (2020)

PURPOSE

To ensure that information and information systems are adequately protected against damage, loss, and unauthorized use, disclosure or modification.

When information and information systems are protected, the Division is better positioned to: protect the privacy of staff and students; manage risks; preserve resources; enable innovation and provide seamless and integrated educational programming.

All records created in the service of Edmonton Public Schools, regardless of form or creator, are the property of Edmonton Public Schools. Records are an asset and support the Division's work in providing a quality education to each student to reach their maximum potential.

DEFINITIONS

Division information is data in any form (physical or digital, in transmission or stored) created or captured for the purpose of Edmonton Public Schools activities in line with the Division's educational mandate and Mission, Vision and Priorities.

Information security is the protection of information from losses of:

- Confidentiality: Information must not be disclosed, purposefully or inadvertently, to anyone who does not have authority to receive it.
- Integrity: Information needs to be accurate and complete.
- Availability: Information must be available when required.

POLICY

The Board is committed to a Division-wide, systematic and coordinated approach to ensuring the confidentiality, integrity and availability of Division information assets in order to support the Division's work in providing a quality education to students in a safe and secure learning environment. The Board believes that the Division's approach to information security should be consistent with international standards, should enable business and educational outcomes, and expects the following principles to guide this work:

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

EXPECTATIONS

1. The Superintendent of Schools shall ensure implementation of this policy through appropriate administrative regulations, defined and communicated processes, practices, and assignment of roles and responsibilities.

2. The Superintendent of Schools shall notify the Board of Trustees of any significant breaches of information security in a timely fashion.

ACCOUNTABILITY

1. A yearly report of information security actions and issues regarding confidentiality, integrity and availability shall be completed internally, and a report of the findings presented to the Board as part of the Division's annual results review.

2. An external audit of information security shall be completed every four years, and a report of the findings presented to the Board of Trustees.

REFERENCES

CN.BP - Managing Division Information
CN.AR - Creation, Use and Maintenance of Division Information
CNA.AR - Security of Personal and Division Information
HO.AR - Student Records
DK.BP - Division Technology
Freedom of Information and Protection of Privacy Act

Education Act
ISO/IEC 27001:2005
Provincial Approach to Student Information (PASI) Usage Agreement
Student Record Regulation of Alberta