Administrative Procedure 124 INFORMATION AND TECHNOLOGY SECURITY

East Central Alberta Catholic School Division believes that standards for protecting information and technology resources must be in place to provide a safe, respectful, and secure learning and working environment that ensures privacy, confidentiality, integrity, and accountability.

All staff using Division information, whether at a Division location or otherwise, are responsible for the management and safekeeping of information under their custody or control. Reasonable administrative, technical, and physical safeguards must be used to prevent unauthorized access, collection, use, disclosure, alteration, loss, or disposal of information. This Administrative Procedure aligns with The Access of Information Act (ATIA), supporting transparency, accountability, and lawful public access to records, and The Protection of Privacy Act (POPA) / Freedom of Information and Privacy Act, establishing standards for the lawful collection, use, disclosure, and safeguarding of personal information.

Definitions

Personal Information – Recorded information about an identifiable individual, including but not limited to names, contact information, biometric data, educational, financial, or employment history, and opinions about the individual.

Protected Information - All information assets in the custody or under the control of the Division that, if compromised, could reasonably result in harm to an individual or to the Division. This includes personal, sensitive, confidential, and operational information.

Portable Technology / Mobile Device – Any portable electronic device capable of storing or transmitting information, including laptops, tablets, smartphones, USB drives, memory sticks, external hard drives, and similar devices.

Privacy Impact Assessment (PIA) – A documented review of how personal information is collected, used, disclosed, stored and safeguarded, conducted prior to adopting new technologies, systems, services, or processes involving personal information.

Procedure

1. Information Security Principles

1.1. Access and Confidentiality – Only authorized persons may access Division information. All information must be maintained in confidence disclosed only where authorized by legislation, regulation, or lawful authority.

1.2. Safekeeping Responsibilities – Each employee is responsible for protecting information under their control by ensuring reasonable security arrangements are in place to prevent unauthorized access, collection, use, disclosure, modification, or disposal.

1.3. Principle of Least Privilege – Users shall be granted access only to the minimum information and systems required to perform assigned job duties.

2. Collection and Use of Information

2.1. Limitation of Collection – The collection of personal information is limited to what is necessary for:

2.1.1. Educational programming and student services

2.1.2. Division operations and administration

2.1.3. Student and staff safety

2.1.4. Compliance with statutory obligations

2.2. Privacy Impact Assessments – A Privacy Impact Assessment must be completed and approved by the Superintendent or designate prior to the use of any new technology, software application, cloud-based service, or process that collects, stores or processes personal information.

2.3. Consent – Explicit consent is required for optional applications or services that:

2.3.1. Collect sensitive personal information;

2.3.2. Store personal information outside of Canada without adequate safeguards, or

2.3.3. Present elevated privacy, security, or reputational risks.

3. Artificial Intelligence (AI)

The Division will not use Artificial Intelligence systems as the sole basis for decisions that significantly affect students (e.g. grading, discipline, placement, or eligibility for services) without meaningful human review. AI use must be transparent, documented, and privacy-assessed.

4. Portable Technology and Mobile Devices

4.1. Device Security – All password protection, screen locking, and security mechanisms available on portable technology must be enabled and used consistently.

4.2. Encryption – Files containing personal, sensitive, or confidential information stored on portable technology must be encrypted or protected using equally strong security measures.

4.3. Personal Devices – Staff shall not store Division information on personally owned devices unless explicitly authorized. Division information must not be copied, downloaded, or retained beyond what is required to perform assigned duties.

4.4. Minimization of Data – Only the minimum information necessary for a specific task may be copied, printed, transported, or stored on portable devices. Information no longer required must be promptly removed.

4.5. Loss or Theft – If a portable device containing Division information is lost or stolen, the employee must immediately notify their supervisor and the Access and Privacy Officer so the Division can assess risk and meet notification obligations.

5. Passwords and Authentication

5.1. Password Strength

5.1.1. Minimum password length: 8 characters

5.1.2. Account lockout: Users are allowed a maximum of five (5) incorrect password attempts before the Active Directory account is automatically locked.

5.1.3. Password complexity: A combination of uppercase letters, lowercase letters, numbers, and special characters.

5.2. Password protection – Passwords must never be written down, shared, or stored in an unencrypted format.

5.3. Multi-Factor Authentication (MFA) – Where available, multi-factor authentication is mandatory for employee access to Division systems and cloud based services.

5.4. Password Changes – User-level passwords must be changed regularly, at least every 120 days, or immediately if compromise is suspected.

6. Secure Storage and Disposal

6.1. Physical Security – Personal, sensitive, or confidential information must not be left unattended in areas accessible to the public unless secured (e.g. locked drawers, cabinets, or rooms).

6.2. Workstation Security – Users must lock or log out of workstations when leaving them unattended.

6.3. Disposal of Information and Equipment – Information no longer required must be transferred to secure storage or destroyed in accordance with records management procedures.

6.3.1. Paper records must be securely shredded

6.3.2. Digital records must be permanently deleted.

6.3.3. Hard drives from printers and photocopiers must be removed and destroyed prior to equipment removal from Division sites.

6.3.4. All obsolete hardware must be wiped of data prior to disposal.

7. Remote Access and Email

7.1. Remote Access Security – Employees accessing Division systems remotely are responsible for ensuring connections are secure, approved, and protected.

7.2. Email Use – Division email must not be used to transmit offensive content. Caution must be exercised when sending personal or confidential information, such information must not be transmitted unless encrypted or otherwise secured.

7.3. Custody and Control of Email – All email sent or received through Division email systems is under the custody and control of the Division and may be subject to access requests under ATIA.

8. Privacy Breach Protocol

8.1. Immediate Reporting – Any suspected or actual loss or breach of personal information must be reported immediately to the employee's supervisor and the Secretary-Treasurer. The Secretary-Treasurer will notify the OIPC in the event of a breach that effects a large number of individuals and/or contains sensitive data.

8.2. Preservation of Evidence – No action may be taken that could impede an investigation, including deleting or altering data, unless directed by the Superintendent or designate.

8.3. Notification – The Division is responsible for assessing risk and notifying affected individuals where a breach presents a reasonable risk of harm.

8.4. Mitigation and Prevention – Root cause analysis, corrective actions and documentation are to be completed.

9. Professional Development and Cybersecurity Awareness

9.1. Mandatory Cybersecurity Training – All employees must participate in ongoing, mandatory cybersecurity awareness training as a condition of continued access to Division information systems.

9.2. Risk Based Rationale – Cybersecurity training supports risk mitigation identified through insurance, operational, and threat environment reviews.

9.3. Cybersecurity Intervention Plan – The Division's cybersecurity program is intendent to:

9.3.1. Reduce the likelihood and impact of cyber incidents;
9.3.2. Increase staff awareness of evolving threats;
9.3.3. Strengthen administrative, technical, and human safeguards; and
9.3.4. Reinforce shared responsibility for protecting Division information assets.

9.4. Approved Training Program – The Division utilizes CIRA Cyber Awareness Training, including surveys, online modules, and refresher training as directed.

9.5. Monitoring and Compliance – Training completion will be monitored. Failure to complete required training may result in restricted system access.

9.6. Annual training covering key concepts in privacy for all staff by completing the Overview of Alberta's Protection of Privacy Act course and Overview of Alberta's Access to Information Act course provided by the Government of Alberta.

Created: January 2026

References: Education Act
Access to Information Act (ATIA)
Protection of Privacy Act (POPA) / Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Copyright Act
Criminal Code of Canada