

Alberta Classical Academy Privacy Management Program

1. Background

Management Program is designed to meet the requirements for public bodies under the Protection of Privacy Act (POPA)¹ and the Protection of Privacy (Ministerial) Regulation², using the OIPC Alberta “Guidance for Public Bodies in Developing Privacy Management Programs” (April 2026).

A copy of this PMP will be made available to any person upon request in accordance with POPA section 25(3) and is available on ACA’s website.

A Glossary of Terms corresponding to this PMP is attached as Schedule “A”.

2. Purpose

The purpose of this Privacy Management Program (“PMP”) is to establish, implement, maintain, review, assess, and continuously improve a comprehensive operational privacy governance framework for Alberta Classical Academy (“ACA”).

This PMP is supported by a series of policies, procedures, forms, templates, inventories, logs, training programs, and governance activities. Together, these documents establish how privacy requirements are implemented in practice throughout the ACA.

This PMP is intended to:

- promote compliance with POPA and ATIA;
- support accountability and transparency;
- protect personal information in the custody or under the control of the Academy;
- operationalize privacy and access obligations across the organization;
- and foster a culture of responsible information stewardship.

This PMP is not intended to operate solely as a collection of policies and procedures. Rather, it is intended to function as an active, operational accountability framework integrated into the ACA’s governance, decision-making, educational operations, technology management, procurement practices, and daily activities.

The ACA will regularly review, monitor, and revise the PMP to ensure it remains effective, current, and responsive to evolving legal, operational, and technological requirements.

¹ *Protection of Privacy Act*, SA 2024, c P-28.5 [POPA], s. 25.

² *Protection of Privacy (Ministerial) Regulation*, Alta Reg 143/2025 [POPA M-Reg.], s. 6.

3. Organizational Commitment

The ACA recognizes that privacy accountability begins with organizational leadership and institutional commitment.

The ACA's Secretary-Treasurer shall:

- actively support this PMP;
- allocate appropriate financial, human, and technical resources;
- support the designated Privacy Officer;
- ensure privacy considerations are integrated into strategic and operational decision-making;
- support ongoing training and awareness;
- oversee material privacy risks and incidents;
- and promote a culture of privacy, confidentiality, transparency, and accountability.

The ACA recognizes that privacy protection is essential to maintaining trust with:

- students;
- parents and guardians;
- employees;
- volunteers;
- contractors;
- the broader school community; and
- the general public.

4. Scope

This PMP applies to:

- all ACA employees;
- teachers;
- administrators;
- contractors;
- consultants;
- volunteers;
- Board members;
- service providers;
- and any third parties acting on behalf of the ACA.

The PMP applies to all personal information in any format within the ACA's custody or control, including:

- student records;
- educational records;
- behavioural records;
- counselling and support information;
- parent and guardian information;

- employee records;
- financial information;
- digital learning systems;
- surveillance systems;
- email systems;
- surveys;
- websites/portals;
- and cloud-based platforms.

5. Risk-Based Privacy Governance

The ACA shall apply a risk-based and proportionate approach to privacy governance consistent with POPA and applicable regulations. Privacy controls, safeguards, monitoring activities, oversight measures, and review mechanisms shall be proportionate to:

- the volume of personal information processed;
- the sensitivity of the information;
- the number of individuals affected;
- the use of service providers and third parties;
- the complexity of the technology, systems, or processes involved; and
- the potential harms associated with unauthorized access, use, disclosure, loss, alteration, or compromise of personal information.

The ACA recognizes that it processes a high volume of highly sensitive personal information, including information relating to minors, educational supports, behavioural matters, and employee information. As a result, the ACA shall implement enhanced privacy governance, safeguards, monitoring, and oversight measures appropriate to the nature of the personal information in its custody or under its control.

The ACA shall proactively monitor information systems containing personal information to help identify, prevent, detect, investigate, and respond to privacy and security risks. Monitoring activities may include audits, access reviews, logging, system alerts, security reviews, and other measures appropriate to the risks presented by the information and systems involved.

Where the ACA creates, uses, or discloses non-personal data, de-identified information, anonymized information, synthetic data, or data derived from personal information, the ACA shall implement appropriate governance, safeguards, and review processes to ensure compliance with POPA and applicable regulations.

Where appropriate, the ACA may utilize additional risk assessment tools, including PIAs, Security Threat and Risk Assessments (STRAs), Algorithmic Impact Assessments (AIAs), and other governance processes to identify, assess, and mitigate privacy, security, fairness, and compliance risks associated with new or modified programs, technologies, systems, and information-sharing activities.

6. Layered Program Controls

The ACA's PMP shall consist of layered organizational controls designed to operate collectively to support privacy compliance and accountability.

These layered controls include:

- governance controls;
- policy controls;
- operational procedures;
- technical safeguards;
- physical safeguards;
- administrative safeguards;
- contractual controls;
- training and awareness;
- monitoring and audit activities;
- privacy impact assessments;
- and incident response mechanisms.

7. Privacy Governance Structure

7.1 Privacy Officer

The ACA head shall designate a Privacy Officer responsible for overseeing compliance with POPA and ATIA. The Privacy Officer will report directly to the Superintendent of Schools.

The Privacy Officer shall:

- oversee the implementation, administration, and ongoing maintenance of the PMP;
- develop, implement, and periodically review privacy policies, procedures, and other program controls;
- monitor and assess the ACA's compliance with POPA and related privacy requirements;
- coordinate responses to access requests and privacy-related inquiries;
- oversee the identification, investigation, management, and notification and reporting of privacy incidents and breaches;
- coordinate PIAs and provide privacy advice on new or modified programs, services, initiatives, and technologies;
- oversee privacy due diligence and reviews relating to service providers, contractors, and third parties;
- develop and deliver privacy training, education, and awareness initiatives;
- monitor, document, evaluate, and report on the effectiveness of the PMP, including conducting audits and compliance reviews as appropriate;
- act as the primary liaison with the OIPC and represent the ACA during privacy investigations, reviews, and inquiries; and
- work with senior leadership to promote and foster a culture of privacy, accountability, and responsible information management throughout the organization.

The Privacy Officer shall have:

- sufficient authority;
- direct access to senior leadership;

- and adequate financial, human, and technical resources necessary to fulfill their responsibilities.

7.2 Leadership Oversight

The Chief Financial Officer and Secretary-Treasurer shall:

- receive periodic privacy compliance reporting;
- review significant privacy incidents and risks;
- monitor remediation activities;
- and oversee implementation of corrective actions where necessary.

8. Personal Information Inventory and Records Governance

In accordance with section 57 of POPA, the ACA shall maintain a comprehensive and current inventory of the personal information in its custody or under its control ("Personal Information Inventory").

The Personal Information Inventory supports the ACA's compliance with POPA and assists the ACA in:

- identifying the personal information it collects, uses, discloses, retains, and manages;
- maintaining its Personal Information Bank ("PIB") directory;
- supporting PIAs, risk assessments, and privacy incident response activities;
- applying appropriate information security classifications and safeguards; and
- supporting records management, accountability, and transparency obligations.

The ACA shall maintain a documented information classification framework that classifies personal information, data derived from personal information, and non-personal data according to sensitivity and risk. Administrative, technical, and physical safeguards shall be applied in a manner proportionate to the assigned classification.

The ACA shall also maintain a PIB directory in accordance with POPA. The PIB directory shall provide a general description of:

- the personal information maintained by the ACA;
- the categories of individuals to whom the information relates;
- the authority for collection;
- the purposes for which the information is collected, used, and disclosed; and
- the location of the PIB.

The Personal Information Inventory and PIB directory shall be reviewed and updated periodically to reflect changes to the ACA's programs, services, systems, information holdings, technologies, and information-sharing activities.

The ACA shall maintain a documented Information Classification Framework that classifies personal information, data derived from personal information, and non-personal data according to sensitivity and risk. Administrative, technical, and physical safeguards shall be applied in a manner proportionate to the assigned classification.

The Information Classification Framework shall be reviewed periodically and updated as necessary to reflect changes in legal requirements, technology, information holdings, and operational practices.

9. Collection, Use, and Disclosure of Personal Information

The ACA shall only collect, use, and disclose personal information:

- where authorized by law;
- where reasonably necessary for educational or operational purposes;
- or where otherwise permitted under applicable legislation.

The ACA shall apply the principle of minimum necessary access and disclosure.

The ACA primarily collects, uses, and discloses personal information under statutory authority and educational mandates. Where consent is required by law or otherwise relied upon by the ACA, the ACA shall maintain documented consent management procedures. Such procedures shall address how consent is obtained, documented, recorded, managed, and withdrawn across oral, written, and electronic interactions. Where highly sensitive personal information is involved, the ACA shall take reasonable steps to ensure that consent is informed and meaningful by providing individuals with clear and understandable information regarding the collection, use, disclosure, and management of their personal information.

Collection notices shall identify:

- the legal authority for collection;
- the purpose of collection;
- and contact information for questions, and
- where applicable, any consent requirements relating to the collection, use, or disclosure of personal information.

10. Access to Information (ATIA) Compliance

The ACA shall maintain operational procedures for responding to access requests under ATIA.

These procedures shall include:

- request intake;
- identity verification;
- records searches;
- exemptions analysis;
- redaction;
- timelines management;
- extensions;
- response preparation;
- and complaint handling.

The ACA shall maintain access request logs and records of decision-making.

11. Information Security Safeguards

The ACA shall implement reasonable administrative, technical, and physical safeguards to protect personal information against unauthorized access, use, disclosure, destruction, or loss.

Safeguards shall include:

- role-based access controls;
- multi-factor authentication;
- encryption;
- endpoint protection;
- logging and monitoring;
- secure backups;
- secure storage;
- visitor management;
- confidentiality agreements;
- and acceptable use requirements.

Safeguards shall be periodically assessed and updated based on evolving risks.

12. Enhanced Controls for Sensitive Personal Information

Because the ACA processes a high volume or highly sensitive personal information concerning minors and educational records, the ACA shall implement enhanced safeguards and oversight measures, including:

- enhanced access controls;
- periodic access reviews;
- elevated vendor due diligence;
- mandatory PIAs for higher-risk initiatives;
- enhanced monitoring;
- enhanced breach escalation procedures;
- and specialized training for high-risk roles.

13. Privacy Impact Assessments (PIAs)

The ACA shall maintain procedures for identifying, completing, reviewing, and, where required, submitting PIAs in accordance with POPA and applicable regulations.

A PIA is a risk assessment tool used to identify and address privacy risks associated with a program, service, initiative, technology, system, or information-sharing arrangement that involves personal information. Consideration of whether a PIA is required shall form part of the planning, procurement, implementation, modification, and review of activities involving personal information.

The ACA shall assess whether a PIA is required whenever it proposes to introduce a new activity or make a significant change to an existing activity involving personal information. Examples of initiatives that may require a PIA include:

- educational technology platforms;
- artificial intelligence and machine learning systems;
- surveillance and monitoring systems;
- cloud-based services and applications;
- automated decision-making tools;
- student monitoring technologies;
- information-sharing initiatives; and
- significant changes to existing programs, services, systems, or technologies involving personal information.

The ACA's Personal Information Inventory and security classification framework shall assist in identifying activities that may require a PIA. ACA staff are expected to consult the Privacy Officer at an early stage of any project, procurement, initiative, or significant change involving personal information so that privacy requirements, including the need for a PIA, can be assessed.

The ACA shall utilize the OIPC's PIA Submission Assessment Tool, OIPC POPA PIA Template and related guidance materials when determining whether a PIA is required, preparing a PIA, and assessing whether submission to the Commissioner is required. Where required by POPA or applicable regulations, completed PIAs shall be submitted to the Office of the Information and Privacy Commissioner.

14. Service Providers and Third-Party Management

The ACA remains accountable for personal information in the custody or under the control of service providers acting on its behalf.

The ACA shall implement:

- vendor due diligence procedures;
- privacy and security contract standards;
- breach notification obligations;
- confidentiality requirements;
- audit rights;
- retention and destruction obligations;
- and cross-border data assessments where applicable.

Vendor relationships involving higher-risk processing shall undergo enhanced review and monitoring.

15. Privacy Incident and Breach Management

The ACA shall maintain documented procedures for identifying, reporting, escalating, containing, investigating, documenting, and responding to privacy incidents.

All ACA personnel are responsible for promptly reporting suspected privacy incidents to their supervisor or the Privacy Officer in accordance with ACA procedures.

All personnel shall immediately report:

- unauthorized access;
- unauthorized disclosure;
- lost devices;
- phishing incidents;
- suspected breaches;
- ransomware events;
- or improper information sharing.

The ACA's incident response framework shall include:

1. Identification
2. Escalation
3. Containment
4. Investigation
5. Harm assessment
6. Notification analysis
7. Remediation
8. Documentation
9. Lessons learned review

The ACA, through its Privacy Officer, will periodically review, evaluate, and test its Privacy Incident and Breach Management procedures to assess their effectiveness and readiness. These reviews may include tabletop exercises, post-incident assessments, and other testing activities designed to evaluate how effectively privacy incidents are identified, escalated, contained, investigated, and managed. The ACA will assess the timeliness with which incidents are detected, the efficiency of internal reporting and decision-making processes, the effectiveness of containment measures, and compliance with applicable obligations under POPA. Lessons learned from these reviews and any actual privacy incidents will be used to strengthen procedures, training, safeguards, and other components of the PMP on an ongoing basis.

16. Privacy Training and Awareness

The ACA shall maintain mandatory privacy and security training programs appropriate to employee roles and responsibilities. Privacy training shall be provided within a reasonable period following commencement of employment or engagement and whenever material changes to privacy requirements occur.

Training shall include:

- onboarding privacy training;
- annual refresher training;
- phishing and cybersecurity awareness;
- access request handling;

- incident response;
- records handling;
- and specialized training for high-risk roles.

The ACA shall maintain records demonstrating completion of required training.

17. Demonstrating Compliance

The ACA shall maintain sufficient documentation and records to demonstrate compliance with POPA, ATIA, and this PMP.

Documentation may include:

- policies and procedures;
- consent records;
- training records;
- PIAs;
- breach logs;
- access request logs;
- audit reports;
- vendor assessments;
- governance records;
- risk assessments;
- and remediation activities.

The ACA acknowledges that accountability requires the ability to demonstrate operational compliance.

18. Monitoring, Auditing, and Metrics

The ACA shall periodically assess the effectiveness of its PMP through:

- audits;
- policy reviews;
- access log monitoring;
- incident trend analysis;
- vendor reviews;
- training reviews;
- and risk assessments.

The ACA shall develop privacy metrics and indicators, which may include:

- training completion rates;
- breach frequency and severity;
- access request response times;
- vendor review completion rates;
- audit findings;

- and remediation completion rates.

19. Ongoing Assessment and Continuous Improvement

The ACA shall establish and maintain a formal process for the periodic review, assessment, and continuous improvement of this PMP.

The PMP shall be reviewed:

- annually;
- following significant privacy incidents or breaches;
- following material legislative, regulatory, or policy changes;
- following significant organizational, operational, or technological changes;
- after implementation of major technologies or information systems; or
- where deficiencies, risks, or opportunities for improvement are identified.

The review process shall take into account information obtained through monitoring activities, audits, risk assessments, privacy incidents, complaints, access requests, training activities, vendor reviews, and reports provided by the Privacy Officer. Where appropriate, the ACA shall update its Personal Information Inventory, policies, procedures, safeguards, privacy notices, and other program controls to address identified risks, operational changes, lessons learned, and evolving legal requirements.

Corrective actions, remediation activities, and improvement initiatives shall be documented and tracked to completion.

20. Transparency and Public Access

Consistent with POPA requirements, the ACA shall make this PMP publicly available upon request or otherwise make it accessible through appropriate public channels.

The ACA shall maintain publicly accessible privacy notices describing:

- how personal information is collected, used, disclosed, retained, and protected;
- how individuals may request access or correction;
- and how privacy concerns may be raised.

Individuals may submit privacy-related complaints to the Privacy Officer in accordance with the ACA's Privacy Complaint Procedures.

21. Privacy by Design and Privacy by Default

The ACA shall integrate privacy by design and privacy by default principles into:

- procurement;
- technology implementation;
- educational programming;
- operational planning;

- and strategic initiatives.

Privacy considerations shall be evaluated at the earliest possible stage of planning and throughout the lifecycle of systems and initiatives involving personal information, including emerging technologies, artificial intelligence, automated decision-making systems, and data analytics tools where applicable.

22. Supporting Policies, Procedures, and Tools

The ACA shall maintain and periodically review policies, procedures, forms, templates, logs, and other supporting documentation necessary to implement and support this PMP and to comply with POPA and its regulations.

A current inventory of the ACA's supporting privacy-related policies, procedures, forms, templates, logs, and governance documents is attached as Schedule "B". Schedule "B" may be updated from time to time without requiring amendment of this PMP, provided the updates remain consistent with the objectives and requirements of this PMP.

The ACA may develop, amend, consolidate, or retire supporting policies, procedures, forms, templates, and tools from time to time to reflect changes in legal requirements, operational practices, technology, organizational structure, emerging privacy risks, and lessons learned through privacy incidents, complaints, audits, investigations, and ongoing reviews of the PMP.

23. Approval and Accountability

This PMP is approved by ACA's Chief Financial Officer and Secretary-Treasurer and shall remain in force until amended or replaced. The ACA acknowledges that effective privacy governance requires ongoing operational commitment, oversight, assessment, and continuous improvement.

The ACA shall establish and document privacy-related roles, responsibilities, and accountabilities throughout the organization. While the Privacy Officer is responsible for overseeing the implementation and administration of the PMP, privacy compliance is a shared responsibility of all employees, contractors, volunteers, and individuals who collect, use, disclose, retain, access, or otherwise handle personal information on behalf of the ACA. Privacy responsibilities may be assigned through policies, procedures, delegation instruments, job descriptions, training materials, and other governance documents, as appropriate.

The ACA may maintain separate delegation instruments, authorization schedules, or operational governance documents identifying individuals authorized to exercise specific privacy-related decision-making powers under POPA, ATIA, this PMP, and associated policies and procedures.

The ACA shall maintain a clear chain of accountability for the protection of personal information, with responsibility flowing from individual personnel to managers, senior leadership, and ultimately the Superintendent of Schools through the Chief Financial Officer and Secretary-Treasurer. The ACA shall periodically review and update its privacy governance framework, delegated responsibilities, and supporting documentation to ensure they remain effective, current, and aligned with POPA, its regulations, and the ACA's operational activities.

To support the accountability requirements of POPA and this PMP, the ACA shall maintain a Privacy Governance and Accountability Framework attached as Schedule “C”, setting out privacy-related roles and accountabilities within the ACA.

The Privacy Governance and Accountability Framework forms part of this PMP and is intended to document the allocation of privacy accountability. Schedule “C” shall be reviewed and updated periodically to ensure it remains accurate, current, and reflective of the ACA's organizational structure and operational activities.