PRIVACY IMPACT ASSESSMENTS (PIA)

BACKGROUND

Westmount Charter School (WCS) recognizes the importance of protecting personal information and maintaining responsible, transparent, and secure information management practices. As a public body under Alberta legislation, WCS is required to collect, use, disclose, retain, protect, and provide access to personal information in accordance with the *Access to Information Act* (ATIA) and the *Protection of Privacy Act* (POPA).

WCS recognizes that new technologies, educational tools, digital platforms, Artificial Intelligence (AI) applications, cloud-based services, and operational initiatives may introduce privacy, security, and legal risks involving personal information. Privacy Impact Assessments (PIAs) support responsible decision-making by identifying, assessing, and mitigating privacy risks before implementation.

WCS recognizes that responsible privacy practices support safe and effective learning environments, student well-being, staff operations, and informed educational decision-making. This Administrative Procedure is intended to support the implementation of Administrative Procedure 170 - Access to Information and Protection of Privacy and Administrative Procedure 172 - Collection, Use, and Disclosure of Personal Information by establishing requirements for Privacy Impact Assessments (PIAs) for initiatives involving personal information.

WCS is committed to a privacy-by-design approach, ensuring privacy considerations are embedded into the planning, procurement, implementation, and ongoing use of programs, technologies, systems, and operational practices involving personal information.

The Superintendent is responsible for implementing this Administrative Procedure.

PRINCIPLES

1. Westmount Charter School shall:

    1.1. Conduct Privacy Impact Assessments (PIAs) where required to identify, assess, and mitigate privacy risks associated with initiatives involving personal information.

    1.2. Apply privacy-by-design principles, ensuring privacy considerations are integrated into the planning, development, procurement, implementation, and review of systems, technologies, and operational practices.

    1.3. Limit the collection, use, disclosure, and retention of personal information to what is reasonable, necessary, proportionate, and authorized by legislation.

    1.4. Ensure reasonable administrative, physical, and technological safeguards are in place to protect personal information.

    1.5. Promote transparency, accountability, and responsible information management practices.

    1.6. Assess privacy risks before implementing initiatives involving new technologies, Artificial Intelligence (AI), educational technology (EdTech), cloud-based systems, third-party

vendors, or significant changes to information management practices or data-sharing practices.

1.7. Ensure privacy risks are considered alongside educational, operational, legal, cybersecurity, student safety and well-being, and instructional considerations.

PROCEDURES

1. Circumstances Requiring a Privacy Impact Assessment (PIA)

1.1. A Privacy Impact Assessment (PIA) shall be initiated when a school, department, or service area proposes to:

1.1.1. Implement new software, applications, databases, or digital platforms involving personal information;

1.1.2. Adopt educational technology (EdTech) tools, student learning applications, or cloud-based services;

1.1.3. Engage third-party vendors or service providers who may access, collect, store, or process personal information;

1.1.4. Implement surveillance, tracking, monitoring, or biometric technologies;

1.1.5. Introduce Artificial Intelligence (AI), automated decision-making systems, or analytics tools involving personal information;

1.1.6. Significantly modify existing systems, technologies, data-sharing practices, or operational processes involving personal information;

1.1.7. Collect new categories of personal information;

1.1.8. Transfer, process, or store personal information outside Canada;

1.1.9. Share personal information with external organizations where not otherwise authorized through existing procedures.

1.1.10. Implement systems involving student profiling, behavioural analytics, predictive tools, or automated recommendations; or

1.1.11. Implement systems involving monitoring, location tracking, or attendance analytics of students or employees.

1.2. Examples of initiatives that may require a PIA include, but are not limited to:

1.2.1. Learning management systems;

1.2.2. Student wellness or mental health applications;

1.2.3. Online assessment platforms;

1.2.4. Communication applications; and

1.2.5. AI-assisted educational or operational tools.

2. Privacy Impact Assessment Process

2.1. Initial Screening

2.1.1. Before procurement, implementation, or significant modification of an initiative involving personal information, the employee or project sponsor shall complete a Westmount Privacy Impact Assessment (PIA) Intake Form and submit it to the WCS Access and Privacy Office.

2.1.2. The WCS Access and Privacy Office shall determine whether:

2.1.2.1. No PIA is required;

2.1.2.2. A simplified privacy review is sufficient; or

2.1.2.3. A full Privacy Impact Assessment is required.

2.2. PIA Preparation

2.2.1. Where a PIA is required, the employee or project sponsor shall provide relevant documentation, such as:

2.2.1.1. Project description and purpose;

2.2.1.2. Educational, operational, or business rationale;

2.2.1.3. Categories of personal information involved;

2.2.1.4. Data collection, storage, access, use, disclosure, and destruction practices;

2.2.1.5. Vendor or service provider documentation;

2.2.1.6. Data residency and hosting information;

2.2.1.7. Cybersecurity and technical safeguards; and

2.2.1.8. Applicable contracts, agreements, or privacy terms.

2.3. Privacy Risk Assessment

2.3.1.The PIA shall assess:

2.3.1.1. Legislative authority for collection, use, and disclosure;

2.3.1.2. Necessity and proportionality of information collection;

2.3.1.3. Consent requirements;

2.3.1.4. Access controls and user permissions;

2.3.1.5. Vendor and contractual risks;

2.3.1.6. Cybersecurity safeguards;

2.3.1.7. Cross-border data storage or access risks;

2.3.1.8. Retention and destruction practices; and

2.3.1.9. Potential impacts on students, staff, families, and organizational operations.

2.3.2. Privacy risks shall be categorized as low, moderate, high, or critical.

2.4. Risk Mitigation

2.4.1. The employee or project sponsor, in consultation with the WCS Access and Privacy Office, Information Technology Services, and other relevant departments, shall implement reasonable mitigation measures, which may include:

2.4.1.1. Limiting personal information collection;

2.4.1.2. Disabling unnecessary features or permissions;

2.4.1.3. Strengthening access controls;

2.4.1.4. Contractual privacy protections;

2.4.1.5. Retention limitations;

2.4.1.6. Encryption or additional security safeguards; and

2.4.1.7. Student and parent/guardian communication measures.

2.5. Review and Approval

2.5.1. The WCS Access and Privacy Office shall review completed PIAs and determine whether:

2.5.1.1. Risks are adequately mitigated;

2.5.1.2. Additional safeguards are required; or

2.5.1.3. The initiative should not proceed until privacy risks are appropriately mitigated.

2.5.2. Where appropriate, consultation may occur with legal counsel, Information Technology Services, administration, or external privacy experts.

2.5.3. No initiative requiring a PIA shall proceed without appropriate review and approval.

3. Vendor and Procurement Requirements

3.1. All vendors or service providers handling WCS personal information shall:

3.1.1. Sign appropriate privacy, confidentiality, and data protection agreements;

3.1.2. Identify where personal information will be stored or accessed;

3.1.3. Provide privacy breach notification procedures;

3.1.4. Maintain reasonable administrative, technical, and cybersecurity safeguards; and

3.1.5. Comply with ATIA, POPA, and applicable privacy legislation.

3.2. Procurement processes involving systems, tools, technologies, or services handling personal information shall include privacy review requirements.

4. Records Retention

4.1. Completed PIAs and supporting documentation shall be retained securely in accordance with Administrative Procedure 180 - Records Retention and Disposition.

5. Monitoring and Reassessment

5.1. A revised or updated PIA may be required when:

5.1.1. Significant system changes occur;

5.1.2. New functionality is added;

5.1.3. Information management practices change; and

5.1.4. Privacy or security incidents occur.

5.2. The WCS Access and Privacy Office may require periodic reassessment of high-risk systems.

6. Training and Awareness

6.1. WCS shall provide appropriate privacy and PIA awareness and training to administrators, school leaders, project sponsors, Information Technology staff, and employees responsible for implementing systems involving personal information.

Legal Reference:	*Education Act* *Access to Information Act* (ATIA) *Protection of Privacy Act* (POPA)
Cross Reference:	AP-145 Responsible Use of Artificial Intelligence (AI) AP-170 Access to Information and Protection of Privacy AP-172 Collection, Use, and Disclosure of Personal Information AP-180 Records Retention and Disposition
Date of Approval:	June 3, 2026
Date of Revision:	
Due for Review:	June 3, 2029