COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION

BACKGROUND

Westmount Charter School (WCS) recognizes the importance of protecting personal information and maintaining responsible, transparent, and secure information management practices that support student learning, employee operations, organizational effectiveness, and public trust.

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 responsible privacy and information management practices are essential to protecting individual privacy rights, supporting safe and effective educational and workplace environments, and ensuring accountability and transparency in decision-making.

WCS recognizes that personal information may be collected, stored, accessed, used, disclosed, and managed through a variety of systems and technologies, including student information systems, employee records, digital learning tools, cloud-based services, communication systems, Artificial Intelligence (AI) applications, and other educational technologies. WCS is committed to ensuring that these practices align with legislative requirements and support the safe, ethical, secure, and educationally appropriate use of technology.

The Superintendent is responsible for implementing this Administrative Procedure.

PRINCIPLES

1. Westmount Charter School shall:
    1.1. Collect, use, disclose, retain, protect, and provide access to personal information in accordance with the *Access to Information Act* (ATIA), *Protection of Privacy Act* (POPA), and other applicable legislation.
    1.2. Ensure personal information is collected fairly, lawfully, and, wherever reasonable, directly from the individual or parent/guardian, unless otherwise authorized by legislation.
    1.3. Inform individuals of the purpose, legal authority, and contact information related to the collection of personal information, where required.
    1.4. Use personal information only for the purpose for which it was collected, for a consistent purpose, or as otherwise authorized by legislation.
    1.5. Limit disclosure of personal information to circumstances authorized by law or where consent has been obtained.
    1.6. Ensure access to personal information is restricted to authorized individuals who require the information to fulfill their professional responsibilities.
    1.7. Implement reasonable administrative, physical, and technological safeguards to protect personal information from unauthorized access, disclosure, loss, theft, or misuse.

1.8. Take reasonable steps to ensure personal information is accurate, complete, and up to date where necessary for educational, employment, operational, or legal purposes.

1.9. Ensure personal information is retained and securely disposed of in accordance with approved records retention schedules and Administrative Procedure 180 - Records Retention and Disposition.

PROCEDURES

1. Collection of Personal Information

1.1. Westmount may collect personal information where necessary to:

1.1.1. Provide educational programming and student support;

1.1.2. Support student health, safety, and well-being;

1.1.3. Administer employment, payroll, benefits, and personnel processes;

1.1.4. Support governance, legal, operational, and reporting requirements; and

1.1.5. Maintain safe and secure learning and working environments.

1.2. Personal information may be collected through:

1.2.1. Registration and enrollment forms;

1.2.2. Student and employee information systems;

1.2.3. Consent forms and communication tools;

1.2.4. Educational assessments and support documentation;

1.2.5. Approved digital learning tools and platforms;

1.2.6. Employment and human resource processes; and

1.2.7. Security, access, or emergency systems where authorized.

1.3. Notice of Collection

1.3.1. At or before the time of collection, reasonable efforts shall be made to inform individuals of:

1.3.1.1. The legal authority for the collection;

1.3.1.2. The principal purpose(s) for which the information is collected; and

1.3.1.3. The title and contact information of a WCS representative who can answer questions regarding the collection.

2. Use and Disclosure of Personal Information

2.1. Personal information shall only be used or disclosed:

2.1.1. For educational, operational, employment, governance, legal, or safety purposes;

2.1.2. With consent where required;

2.1.3. Where required or authorized by legislation; or

2.1.4. In health, safety, or emergency circumstances.

2.2. Employees and authorized users shall access personal information only where necessary to perform assigned responsibilities.

2.3. Personal information shall not be used or disclosed:

2.3.1. For personal interest or unauthorized purposes;

2.3.2. For commercial or marketing purposes; or

2.3.3. In ways inconsistent with legislative requirements.

3. Educational Technology and Artificial Intelligence (AI)

3.1. Schools shall ensure that approved educational technology (EdTech) tools, digital platforms, cloud services, and Artificial Intelligence (AI) applications align with:

3.1.1. ATIA and POPA requirements;

3.1.2. Educational and operational needs; and

3.1.3. Privacy, confidentiality, and security expectations for third-party service providers or vendors handling personal information.

3.2. Personal information shall not be entered into unapproved digital systems or Artificial Intelligence (AI) platforms unless authorized and aligned with Administrative Procedure 145 - Responsible Use of Artificial Intelligence (AI).

3.3. Employees shall exercise professional judgment when using digital technologies involving student or employee personal information.

4. Privacy Breach Management

4.1. Any actual or suspected privacy breach shall be reported immediately to the employee's supervisor, Principal (where applicable), Superintendent, and/or WCS Access and Privacy Office.

4.2. Westmount shall:

4.2.1. Contain and assess the breach;

4.2.2. Investigate the circumstances and impact;

4.2.3. Notify affected individuals and the Office of the Information and Privacy Commissioner (OIPC), where required; and

4.2.4. Implement corrective actions to reduce the likelihood of recurrence.

5. Staff Responsibilities

5.1. All staff are responsible for:

5.1.1. Protecting confidential and personal information;

5.1.2. Accessing information only as required for their role;

5.1.3. Securely handling physical and digital records;

5.1.4. Complying with ATIA, POPA, and Charter Board procedures; and

5.1.5. Immediately reporting privacy concerns or breaches.

5.2. Principals and supervisors are responsible for supporting staff awareness and compliance with privacy expectations within their areas of responsibility.

5.3. The WCS Access and Privacy Office is responsible for:

5.3.1. Supporting organizational compliance with privacy legislation;

5.3.2. Coordinating access and privacy requests;

5.3.3. Supporting privacy breach management; and

5.3.4. Providing guidance to staff regarding privacy practices.

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-180 Records Retention and Disposition
Date of Approval:	June 3, 2026
Date of Revision:	
Due for Review:	June 3, 2029