Medicine Hat Public School Division
601-1st Avenue SW, Medicine Hat, AB T1A 4Y7 | Phone 403.528.6700 | Fax 403.529.5339 | www.mhpsd.ca

MEDICINE HAT PUBLIC BOARD OF EDUCATION OPERATES AS MEDICINE HAT PUBLIC SCHOOL DIVISION,
AND FOR THE PURPOSE OF THIS DOCUMENT WILL BE REFERRED TO AS "MHPSD" AND/OR "DIVISION"

SECTION 600 – STUDENTS

ADMINISTRATIVE PROCEDURE: VIDEO SURVEILLANCE

PROCEDURE CODE:	*644 AP 001*
Policy Reference: 644 – Surveillance	**Exhibits:** 644 E 001 – Sample Letter for Principals 644 E 002 – Security Camera Installation Request Form 644 E 003 – Notice Signage Template 644 E 004 – Surveillance Video Release Form 644 E 005 – Log: Access and Viewing of Video Surveillance

DEFINITIONS:

1. "**Video Surveillance System**" means a mechanical, electronic or digital device – including IP cameras, network video recorders (NVRs), digital video recorders (DVRs), cloud-managed camera systems, and doorbell or entrance-management cameras - that enables continuous or periodic observing, monitoring, or recording of individuals in school buildings and on school premises.
2. "**Recording"** means any record – whether stored locally, on network-attached media, or in a cloud environment - that is capable of being produced from a machine-readable record.
3. "**Real Time Monitoring**" means the viewing of images when the events shown are actively occurring, whether accessed locally or through remote network access tools.
4. **"Personal Information"** means personal information as defined in the Protection of Privacy Act. (POPA), SA 2024, c P-26.5
5. **"Privacy Impact Assessment (PIA)"** means a structured analysis of the privacy risks associated with a program or system that collects, uses, or discloses personal information, conducted in accordance with POPA and the Division's Privacy Management Program.
6. **Privacy Management Program (PMP)"** means the Division's documented program for managing personal information in compliance with POPA, as required under that Act.

7. **"Data Residency"** means the geographic location where recorded footage and associated metadata are stored and processed.
8. **"Director of Technology"** means the senior technology officer of the Division responsible for cybersecurity, privacy-related technology decisions, and oversight of the Division's information systems.
9. **"Real Risk of Significant Harm (RROSH)"** means the threshold under POPA at which a privacy breach triggers mandatory notification obligations to affected individuals and the Office of the Information and Privacy Commissioner of Alberta (OIPC).

PROCEDURES

1. Use of Video Surveillance Systems:
   1.1. The Board will only collect, use and disclose personal information obtained through a video surveillance system in accordance with the Protection of Privacy Act (POPA) and the Education Act.
   1.2. Video surveillance systems may be used to monitor and/or record activity that occurs on property that is owned, operated or leased by the Division.
   1.3. Before video surveillance is introduced or materially expanded at any site, the school principal must complete the Security Camera Installation Request Form (Exhibit 644 E 002). The form is the standard due diligence record for all new camera installations and captures the information required to assess privacy risk, justify placement, and obtain necessary approvals. Completion of the form does not, by itself, constitute a full Privacy Impact Assessment. The form must be:
      1.3.1. Completed by the school principal or site supervisor;
      1.3.2. Reviewed by the Director of Technology to confirm that technical configuration, cybersecurity controls, and data residency requirements are satisfied; and
      1.3.3. Approved in writing by the Superintendent of Schools before any installation proceeds.
   1.4. A full Privacy Impact Assessment (PIA) is required in addition to the Installation Request Form where the form identifies any of the following elevated risk factors:
      1.4.1. The system will involve sharing personal information with one or more other public bodies (e.g., RCMP, another school division, or a shared services entity);
      1.4.2. The system incorporates AI-enabled analytics (see also section 1:10);.
      1.4.3. Footage will be stored outside Canada;
      1.4.4. The installation represents a material expansion of surveillance coverage at a site where no PIA has previously been conducted; or
      1.4.5. The Director of Technology or Superintendent determines that the scope or sensitivity of the collection warrants a full PIA.

1.5. Where the Installation Request Form identifies that a proposed system involves the sharing of personal information with one or more other public bodies, a full PIA is required and must be submitted to the OIPC in advance of implementation, in accordance with POPA.

1.6. Video surveillance camera locations must be authorized by the Superintendent of Schools or designate. Parents and, where appropriate, students must be informed of surveillance at a site (see Exhibit 644 E 001 – Sample Letter for Principals).

1.7. Surveillance cameras located inside a building shall not be directed to look through windows to areas outside the building, unless necessary to protect external assets or to ensure the personal safety of students or employees.

1.8. Cameras shall in no event be directed to look through the windows of adjacent buildings.

1.9. Video surveillance cameras shall not be used to monitor areas where individuals have a reasonable expectation of privacy. Such areas include, change rooms and any discrete toilet or shower areas within washrooms. Common wash areas – including sink and hand-washing areas within gender neutral washrooms – do not carry the same expectation of privacy and may be considered for surveillance where a legitimate safety or security purpose exists and the installation is otherwise authorized under this Procedure.

1.10. Video recordings may be used by the Board or designate as evidence in any disciplinary action arising from an individual's conduct on Board property and/or to detect criminal offences that occur in view of the camera.

1.11. Notice signs must be posted at all surveilled areas and shall disclose (see Exhibit 644 E 003 – Notice Signage Template):

1.11.1. The areas in which surveillance is conducted;

1.11.2. The purpose for the surveillance;

1.11.3. The legal authority for collection under POPA; and

1.11.4. Contact information for the Division's Privacy Officer for additional information.

1.12. Artificial Intelligence and Analytics. Video surveillance systems incorporating AI-enabled analytics including but not limited to facial recognition, behavioural anomaly detection, or occupancy tracking are prohibited unless a dedicated PIA addressing those specific capabilities has been completed, reviewed by the Director of Technology, approved by the Superintendent, and (if applicable) submitted to the OIPC. The Board of Trustees must be informed before any AI-enabled capability is activated.

1.13. Body-Worn Cameras. Body-worn cameras worn by any Division employee or contracted security personnel are subject to this Administrative Procedure in all respects. Their deployment requires completion of the Security Camera Installation Request Form and Superintendent approval. Given the heightened privacy implications of mobile recording, a full PIA is required for all body-worn camera deployments.

2. Installation Request and Privacy Assessment Process

2.1. Security Camera Installation Request Form (Exhibit 644 E 002). The Installation Request Form is required for all new camera installations and material expansions of existing systems. The form must capture, at minimum:

2.1.1. The purpose and justification for the installation, including the specific safety, security, or operational concern being addressed;

2.1.2. Proposed camera placement, field of view, and proximity to any areas of reasonable privacy expectation;

2.1.3. The types of individuals likely to be captured and estimated volume of collection;

2.1.4. Data residency: the geographic location where footage will be stored and whether storage is on-premises, cloud-based, or a hybrid arrangement;

2.1.5. Third-party vendor involvement, including whether any vendor has remote access to the system;

2.1.6. Proposed retention and disposal arrangements; and

2.1.7. Identification of any elevated risk factors that would trigger a full PIA under section 1.3(b).

2.2. Full Privacy Impact Assessment (PIA). Where a full PIA is required under section 1.3(b), it must be:

2.2.1. Initiated using the information captured in the completed Installation Request Form;

2.2.2. Reviewed and approved by the Director of Technology;

2.2.3. Approved by the Superintendent before installation proceeds; and

2.2.4. Submitted to the OIPC where the system involves sharing personal information with another public body.

2.3. Completed Installation Request Forms and any associated PIAs shall be retained by the Director of Technology as part of the Division's Privacy Management Program documentation.

2.4. Material Changes to Existing Systems. Where a material change is made to a system that was installed under a prior Installation Request Form — including camera relocation, system upgrades, changes to data storage location, vendor changes, or addition of AI-enabled capabilities — a new Installation Request Form must be completed. The Director of Technology shall determine whether the change additionally triggers a new or amended PIA under section 1.3(b).

3. Security:
   - 3.1. Installation. Only a designated employee or approved agent of the Division is permitted to install video surveillance cameras. Installation must comply with technical specifications approved by the Director of Technology.
   - 3.2. Access Controls. Access to the surveillance system — including physical access to recording equipment and logical access via network or remote tools — shall be restricted to the school principal or designates and the Director of Technology or designates. All system access must be protected by:
     - 3.2.1. Multi-factor authentication (MFA) for any network-based or remote access to the surveillance system or its management interface;
     - 3.2.2. Unique, non-shared credentials for each authorized user; and
     - 3.2.3. Revocation of access upon change of role or departure from the Division.
   - 3.3. Network Security. Video surveillance systems must be placed on a dedicated or appropriately segmented network. Footage transmission must be encrypted in transit. Default manufacturer credentials must be changed prior to deployment. Firmware and software must be kept current with security patches.
   - 3.4. Remote Access. Remote access to the surveillance system (including via mobile applications or web portals) is permitted only for authorized personnel and must:
     - 3.4.1. Be enabled only with Director of Technology approval;
     - 3.4.2. Use encrypted connections (e.g., VPN or TLS-secured portal);
     - 3.4.3. Require MFA; and
     - 3.4.4. Be logged in the access log (see Exhibit 644 E 005).
   - 3.5. Vendor Access. Where a third-party vendor has technical access to the surveillance system (including for maintenance, cloud storage, or managed services), the Division must:
     - 3.5.1. Execute a Vendor Data Processing Agreement prior to granting access, confirming the vendor's obligations with respect to personal information under POPA;
     - 3.5.2. Confirm that data residency obligations are met (Canadian jurisdiction preferred; any offshore storage requires Director of Technology and Superintendent approval and must be disclosed in the installation Request Form and, where applicable, the PIA); and
     - 3.5.3. Log all vendor access events.
   - 3.6. Storage Security. Video recordings shall be retained in secure storage inaccessible to students and members of the public. All recordings shall be indexed by camera site and date.
   - 3.7. Video recordings may not be disclosed, publicly viewed, or distributed except as authorized by this Procedure or by law.

4. Real Time Monitoring:
   4.1. The principal must approve all instances of real time monitoring. Real time monitoring shall be limited to circumstances where there is a substantial and compelling concern for safety, security or investigation of a specific allegation of significant misconduct.
   4.2. Monitors used for real time monitoring - whether physically located at the site or accessed remotely - shall be accessible only to the principal or a designated authorized employee. Remote real time monitoring is subject to the requirements of section 3 above.
   4.3. All instances of real time monitoring shall be recorded in the access log (see Exhibit 644 E 005), including the date, time, purpose, and name of the authorizing principal.
5. Viewing of Video Recordings:
   5.1. Access Requests by Individuals. An individual whose personal information has been recorded may request access to that information in accordance with POPA. Access requests must be directed to the Division's designated head. Upon receiving an access request, the Superintendent or designate shall:
      5.1.1. Complete a Surveillance Video Release Form (Exhibit 644 E 004) before releasing any footage;
      5.1.2. Document the requester's identity, the date of the recording, the date released, and the date returned (or reason for non-return); and
      5.1.3. Redact or withhold footage identifying third parties where required under POPA, in consultation with the Director of Technology.
   5.2. General Records Requests. Requests for access to records related to the operation of the video surveillance program (other than access to personal information in recordings) are governed by the Access to Information Act (ATIA).
   5.3. Authorized Viewing. Video monitors used to view recordings shall not be located where public viewing is possible. Only employees of the Division authorized to do so in the performance of their duties may review surveillance recordings. All authorized viewing shall be logged (Exhibit 644 E 005).
6. Retention and Disposal of Video Recordings:
   6.1. Default Retention. Video recordings shall be overwritten or otherwise disposed of within 30 days of creation, unless retained under sections 6.2 or 6.3 below.
   6.2. NVR Automated Overwrite. Where a digital video recording system overwrites footage automatically on a loop, this is an acceptable disposal mechanism provided that:
      6.2.1. The overwrite cycle is configured to occur within the 30-day retention period;
      6.2.2. The Director of Technology has confirmed the configuration in writing; and
      6.2.3. Incident-related footage is quarantined prior to the scheduled overwrite when retention is required under this Procedure.

6.3. Extended Retention. Footage may be retained beyond 30 days at the request of the school principal, a Division official, a law enforcement authority, an employee, parent, or student, where the footage relates to a specific incident. Extended retention applies only for the duration reasonably required to resolve that incident.

6.4. Decision Records. Recordings used to make a decision directly affecting an individual shall be retained for a minimum of two years from the date of that decision.

6.5. Legal Proceedings. Where an incident raises the prospect of a legal claim against the Division, the recording or a copy shall be transmitted to Division legal counsel. The original shall be retained until the final conclusion of legal proceedings.

6.6. Secure Disposal. All recordings shall be disposed of securely. Disposal must render the footage unrecoverable, using a method appropriate to the storage medium (e.g., cryptographic erasure for cloud storage, multi-pass overwrite for local digital media, or physical destruction for non-rewritable media). Disposal shall be documented.

7. Privacy Breach Notification

7.1. A privacy breach occurs when footage is accessed, used, disclosed, copied, or disposed of in a manner that is not authorized by this Procedure or by law.

7.2. Upon becoming aware of a potential breach, the school principal must immediately notify the Director of Technology and the Division's Privacy Officer. The Director of Technology shall assess whether the breach creates a real risk of significant harm (RROSH) to one or more individuals.

7.3. Where the RROSH threshold is met, the Division must notify:

7.3.1. Affected individuals in accordance with POPA; and

7.3.2. The OIPC, in accordance with POPA notification requirements.

7.4. All privacy breaches involving video surveillance footage shall be documented and retained as part of the Division’s Privacy Management Program, regardless of whether the RROSH threshold is met.

8. Governance and Review

8.1. Each school principal or site supervisor is responsible for the proper implementation and ongoing operation of the video surveillance system at their site, in accordance with this Procedure.

8.2. The Director of Technology is responsible for:

8.2.1. Technical review and approval of all new and materially modified surveillance installations;

8.2.2. Oversight of cybersecurity controls across all Division surveillance systems;

8.2.3. Maintaining the Division’s inventory of active surveillance systems; and

8.2.4. Retaining completed Installation Request Forms and any associated PIAs as part of the Privacy Management Program.

8.3. All surveillance operations are subject to audit. School principals and site supervisors may be required to justify any aspect of their use of video surveillance.

8.4. This Procedure shall be reviewed at minimum every three years, or sooner upon any material change to applicable legislation, OIPC guidance, or the Division's surveillance technology infrastructure. The Director of Technology shall initiate each review in consultation with the Superintendent.

8.5. The Board of Trustees will take appropriate action in any cases of wrongful use of this Procedure.

9. Law Enforcement Exemption

This Procedure does not apply to covert or overt surveillance equipment being used as a case-specific investigative tool for law enforcement purposes, or as required by law.

REFERENCES

Alberta Education – Education Act
Protection of Privacy Act (POPA)
Access to Information Act
Student Record Regulations
MHPSD Privacy Management Program

Approved: September 7, 2010
Revised: May 11, 2026