



PVNC CATHOLIC ADMINISTRATIVE PROCEDURE	
Administrative Procedure Records and Information Management	Administrative Procedure Number 1201
Directional Policy 1200 - Records and Information	

Title of Administrative Procedure:

Records and Information Management

Date Received:

June 23, 2026

Projected Review Date:

2031

Directional Policy Alignment:

This Administrative Procedure operationalizes Directional Policy 1200 – Records and Information Management. It establishes standard operating procedures to ensure the systematic creation, capture, organization, retrieval, security, tracking, and final disposition of all Board information assets.

Alignment with Multi-Year Strategic Plan:

This procedure supports the Board’s vision—“Rooted in community, formed in faith, ready to change the world”—by ensuring the integrity, security, and accessibility of the data that documents Board transactions, academic progress, and operational decisions.

Modern, compliant information management directly advances the core pillars of our Multi-Year Strategic Plan:

- **Inspire:** By leveraging secure, integrated digital platforms and innovative data practices that cultivate critical thinking and collaborative administrative excellence.
- **Thrive:** By establishing fair expectations, consistent data workflows, and corporate accountability to maintain safe, respectful, and legally compliant information environments.
- **Connect:** By promoting well-being, data privacy, and digital equity, ensuring that staff and student information is securely handled and valued in mind, body, and spirit.

[PVNCCDSB Board Vision, Mission and Strategic Priorities](#)

Background:

At the foundation of the Board's records management program is the General Records and Retention System (GRRS). The GRRS acts as the definitive legal and operational authority governing Board data lifecycles. It maps out a systematic, functional arrangement of information assets and dictates the mandatory minimum periods a record must be maintained based on federal and provincial statutes, fiscal requirements, and administrative utility.

All staff can access the master digital version of the GRRS via the internal employee dashboard.

Action Required:

1.0 General

- 1.1 The Board shall maintain a comprehensive records and information management program that complies with the *Education Act* and its accompanying regulations, the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and all other applicable federal and provincial legislation governing data preservation, security, and retention periods for all Board information holdings.
- 1.2 This Administrative Procedure applies to all records within the custody or under the control of the Peterborough Victoria Northumberland and Clarington (PVNC) Catholic District School Board related to any and all Board business. This mandate applies regardless of the physical medium

or digital platform in which those records are created, stored, or maintained—explicitly including paper documents, on-premises servers, board-sanctioned cloud environments (e.g., Google Workspace, Microsoft 365), collaboration software, and portable devices.

- 1.3 All Board documents and data structures must be retained in strict accordance with the dynamically maintained General Records and Retention System (GRRS).
- 1.4 Individual departments and schools hold direct operational responsibility for the management, organization, and tracking of records and information relevant to their unique functions in full compliance with the GRRS. This responsibility extends to all data generated within specialized, department-specific software applications and cloud-hosted platforms.
- 1.5 The Records and Information Management Department—acting in strategic coordination with Information Technology Services—is responsible for providing secure storage and retrieval infrastructures for inactive records. Together, they shall oversee corporate record-keeping systems, automated lifecycle configurations, and services that effectively maintain and retrieve information in compliance with the GRRS.
- 1.6 All Board records shall be efficiently and systematically disposed of or permanently purged in accordance with the timelines established by the GRRS. Disposal occurs upon the documented authority of the designated record owner once administrative, legal, and fiscal values have ceased. All legislative requirements must be fully met, while ensuring the permanent preservation of records possessing enduring archival, historical, or vital value to the Board.
- 1.7 All records scheduled for disposal that contain confidential or personal information must be destroyed in a secure, irreversible, and permanent manner. This requires the physical shredding of paper documents to prevent reconstruction, or the permanent cryptographic erasure, purging, or overwriting of digital data so it cannot be recovered or reconstructed.
- 1.8 Legal requirements, statutory obligations, and formal corporate Litigation Holds supersede any and all Board policies authorizing the destruction of records, including the authority normally granted via approved retention schedules. Upon issuance of a legal or litigation hold, all automated or manual disposal and deletion activities for affected records must immediately cease until the hold is formally lifted.

2.0 Records and Information Classification and Retention

- 2.1 The Board's General Records and Retention System (GRRS) is the authoritative management tool designed to enable staff to:
 - 2.1.1 Classify documents, data structures, and information for secure filing, tagging, and rapid retrieval based on business function, subject matter, and metadata;
 - 2.1.2 Ensure all information holdings are retained for the precise durations required to satisfy statutory, regulatory, legal, fiscal, audit, historical, or operational requirements;
 - 2.1.3 Systematically manage the lifecycle of records from active use to final disposition in strict accordance with the GRRS; and
 - 2.1.4 Securely delete, purge, or destroy records upon the expiration of their mandated retention periods, utilizing documented manual authorizations or approved automated system workflows from the designated record owner.
- 2.2 The authoritative master version of the GRRS is digitally maintained by the RIM Department. It is accessible to all Board staff via the internal employee dashboard.
- 2.3 The GRRS is a dynamic system that is continuously updated to reflect evolving provincial/federal legislation, regulatory amendments, and Board administrative directives. While Board staff are expected to reference the GRRS when organizing new files or systems, the RIM Department will actively work to integrate these retention rules directly into corporate digital repositories to automate compliance.
- 2.4 The RIM Department shall proactively notify affected departments and roles regarding critical updates, structural changes, or legislative shifts to the GRRS that directly impact their operational responsibilities. These notifications will be issued through formal board communications, targeted training updates, or system-wide release notes.

3.0 Management of Active Records

- 3.1 Active records are information resources currently required to support ongoing Board operations, academic programs, administrative workflows, or active transactions. While typically referenced on a routine daily, weekly, or monthly basis, a record remains "active" as long as the business matter, operational function, or school year to which it relates remains open, unresolved, or ongoing.
- 3.2 Active records must be classified by function, activity, and subject matter at the time of their creation or receipt, in full alignment with the GRRS. Where possible, staff shall utilize board-sanctioned digital repositories

configured to automatically apply these classification rules to ensure appropriate security controls and retention periods are established from the outset.

- 3.3 The Board's classification logic is designed to be functional, flexible, and scalable. It organizes information from broad corporate categories down into increasingly specific operational activities and record types. This structure allows electronic data to be effectively indexed, tagged, and retrieved across all Board platforms.
- 3.4 Staff shall consult Appendix A of this Administrative Procedure, which outlines the subject-based classification scheme configured to mirror the structure of the GRRS, to review the active classification categories, naming conventions, and organizational structures required for their specific school or department records.

4.0 Management of Inactive and Expired Records

- 4.1 Records and information are designated as inactive when their operational lifecycle concludes and the necessity for immediate, routine reference declines, yet they must be preserved to fulfill lingering fiscal, legal, or administrative obligations. Records are designated as expired strictly when the minimum retention period prescribed by the GRRS has been completely satisfied, and no active litigation holds or statutory extensions apply.
- 4.2 The organization, systematic tracking, and management of inactive records must adhere to the following protocols:
 - 4.2.1 **Format-Specific Retention:** Retention periods must be applied uniformly to both physical and digital records in compliance with the GRRS. Physical records must be properly indexed, boxed, and labelled to ensure rapid retrieval. Digital records must be organized within designated archival structures, or tagged with appropriate lifecycle metadata, to prevent data fragmentation. .
 - 4.2.2 **Secure Archival Environments:** Inactive physical records must be transferred to centralized, secure Board storage facilities. Inactive digital records must be maintained in secure, board-sanctioned central electronic repositories or cloud-archival tiers with restricted access controls.
 - 4.2.3 **Defensible and Authorized Disposition:** Obsolete and expired records must be eliminated using environmentally sound, legally compliant, and highly secure destruction or data sanitization methods. This disposal occurs only after all legislative, legal, fiscal,

and operational requirements are satisfied, and final authorization is documented using the designated Board appendix processes.

5.0 Records Disposition

5.1 Records and information holdings shall be handled and disposed of according to their lifecycle status as follows:

5.1.1 If Inactive (Operational Use Has Concluded):

- **Store (Physical):** Official paper records that are no longer regularly referenced but have remaining retention periods must be securely packed, indexed, and transferred to Central Storage facilities. This mandate strictly applies to all physical records designated as Permanent or Archival.
- **Archive (Digital):** Official electronic records that are inactive but possess remaining retention periods must be migrated out of active production environments (such as user inboxes or general shared drives). They must be placed into secure, restricted-access electronic archives or cold cloud storage environments to preserve data integrity and enhance cyber security.

5.1.2 If Expired (Retention Period Completed):

- **Shred (Physical):** Official paper records must be securely shredded once their mandated retention period has expired and the designated record owner has authorized the destruction via written or authenticated digital signature. Stored and shredded physical records must be formally logged, tracked, and audited using the Records Transfer List located in Appendix B.
- **Purge/Sanitize (Digital):** Official electronic records must be permanently purged, cryptographically erased, or overwritten when their retention period is complete so that they cannot be recovered. System-wide deletions and electronic purges shall be permanently tracked and audited using the Disposition Log located in Appendix C to maintain a legally defensible audit trail of destruction.

5.2 **Confidential and Personal Information Records:** Records containing confidential, proprietary, or personal information must be treated with the highest level of security during storage, maintenance, transfer, and final disposal. In strict compliance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), these records must be destroyed or sanitized using specialized methods that guarantee the data cannot be

read, interpreted, intercepted, or reconstructed. Any disposal of physical hardware or digital storage media containing such data must be coordinated with Information Technology Services to ensure absolute data sanitization.

6.0 Historical Archives

- 6.1 A historical archive is a curated collection of historically significant records, data, and memorabilia that document and preserve the rich history, decisions, and evolution of Catholic education within the communities served by the Board.
- 6.2 The GRRS identifies specific record series deemed to possess long-term historical significance. The RIM Department, in collaboration with designated record owners, shall evaluate and assign archival value to records that merit permanent preservation.
- 6.3 Archival records must possess enduring administrative, fiscal, legal, evidential, or cultural values that justify their permanent retention. The archival program ensures that once operational utility ceases, these valuable assets are protected against accidental destruction.
- 6.4 Format-Agnostic Preservation:
 - 6.4.1 **Physical Archives:** Staff must exercise care when handling, indexing, and boxing physical archival materials. Items must be stored in climate-controlled environments with adequate structural descriptions to permit access while minimizing degradation.
 - 6.4.2 **Digital Archives:** Historically significant digital records (including executive minutes, landmark photography, and official publications) must be migrated to secure, long-term preservation formats to ensure they remain readable and uncorrupted as technology evolves.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment of this administrative procedure with the Records and Information Management Directional Policy;
- Reviewing the Records and Information Management Administrative Procedure as part of its regular policy and procedure review cycle.

The Director of Education is responsible for:

- Designating resources for ensuring the implementation of and compliance with this Administrative Procedure.

Superintendents of Schools and System Portfolios are responsible for:

- Ensuring any employee for whom they have supervisory responsibility are compliant with the requirements under this Administrative Procedure.

Principals, Vice-Principals, Managers and Supervisors are responsible for:

- Maintaining effective management of records created and/or used in the school or department in compliance with the GRRS as well as other documents not covered in GRRS.

Manager of Communications is responsible for:

- Overseeing and executing all Freedom of Information (FOI) Access and Correction Requests on behalf of the Director of Education (Head of the Board) in compliance with MFIPPA.
- Issuing formal Litigation Holds to freeze data destruction workflows when an FOI request or legal matter is anticipated or active.

Program Lead of Cybersecurity is responsible for:

- Overseeing the Records and Information Department, the implementation and ongoing operation of the Board's RIM program and compliance with the GRRS.

The Information Governance Specialist is responsible for:

- Maintaining and updating the GRRS.
- Providing relevant staff training on the Board's records and information management program.
- Overseeing the centralized secure storage facilities of board inactive records and the formal process of transferring inactive records from schools/departments to the storage facilities.
- Arrange for confidential destruction of records in accordance with the GRRS.

Staff are responsible for:

- Complying with this Administrative Procedure.
- Understanding their obligations to create and maintain accurate records within the operation of their roles.

Progress Indicators:

- **Reduction of Information Liability (Defensible Deletion):** Measurable annual reduction in the volume of expired digital data and legacy physical records securely purged from active networks and storage facilities, validated by system-generated platform disposition logs.
- **Audit and Compliance Readiness:** Successful completion of annual random RIM compliance reviews across various departments and schools, measuring adherence to the GRRS naming conventions, filing structures, and secure disposal workflows.
- **Litigation Hold Execution Efficiency:** 100% compliance with the immediate preservation and tracking of records whenever a formal corporate Litigation Hold or Freedom of Information (FOI) freeze is issued.
- **Archival Preservation Rate:** Ongoing, systematic transfer and indexing of historically significant physical and born-digital assets into secure, permanent archival environments, preventing historical data gaps.

Definitions:

- **Record:** Any recorded information, regardless of physical form or characteristics, created, received, or maintained by the Board as evidence of its operations, academic programs, legal obligations, or transactions. Records serve as corporate assets and proof that the Board is operating as intended. Recorded formats include paper documents, emails, cloud-hosted files, databases, and audio/visual recordings.
 - **Official Record:** The authoritative, master, or original version of a record (as opposed to a duplicate or convenience copy) to which the retention periods specified in the GRRS must be strictly applied.
 - **Transitory Record:** Information required only for a limited time to complete a routine action or prepare a subsequent record (e.g., working drafts, convenience copies, or temporary notes). Transitory records do not document Board decisions or operations and may be destroyed without formal authorization once their utility ceases.
- **Active Record:** An information asset currently required to support ongoing Board business operations, academic programs, or administrative workflows that is frequently referenced or modified.

- **Inactive Record:** A record that is no longer required for day-to-day operations but must be legally or fiscally preserved for a remaining duration prescribed by the GRRS.
- **Expired Record:** A record that has successfully fulfilled its minimum mandated retention period under the GRRS and is eligible for final disposal or secure purging, provided no active legal restrictions apply.
- **General Records and Retention System (GRRS):** The authoritative master digital system managed by the RIM Department and accessed via the internal employee dashboard. It organizes Board information holdings into functional categories and prescribes the mandatory minimum and maximum timeframes that official records must be retained based on legal, fiscal, and operational requirements.
- **Litigation Hold (Legal Hold):** A temporary, legally mandated directive issued by the Board to freeze regular data-retention schedules. A Litigation Hold strictly prohibits the destruction, deletion, altering, or purging of any physical or digital records relevant to an ongoing or anticipated lawsuit, investigation, or formal freedom of information request.

Appendices:

- [Appendix A - General Records and Retention Schedule \(GRRS\) Scheme:](#) Outlines the organizational and filing logic configured to mirror the structure of the GRRS, assisting staff in correctly indexing and naming records at the point of creation or capture.
- [Appendix B - Records Transfer List:](#) Establishes the mandatory auditing, tracking, and approval workflow required when transferring inactive physical records to centralized storage or certifying the destruction of expired physical documents.
- [Appendix C - Disposition Log:](#) Serves as the official corporate audit trail for tracking and verifying the permanent deletion, purging, or cryptographic erasure of expired electronic datasets.

References:

- [Education Act, R.S.O. 1990, c. E.2](#), section 171 (38) (Powers of Boards: Maintenance and Destruction of Records)
- [Ontario Regulation 298 \(Operation of Schools - General\)](#), under the Education Act (governing Ontario Student Records)

- [Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56 \(MFIPPA\)](#), Section 4(1) (Right of Access) and Section 48(1) (Regulations regarding security and disposal of personal information)
- [Archives and Recordkeeping Act, 2006, S.O. 2006, c. 34, Sched. A](#)
- [Limitations Act, 2002, S.O. 2002, c. 24, Sched. B](#) (governing legal timelines for retaining records subject to potential litigation)
- [Ontario Government Cyber Security Guidelines](#)
- [Directional Policy 1200 – Records and Information Management](#)
- [Administrative Procedure 1202 – Protection of Privacy](#)
- [Administrative Procedure 1207 – Freedom of Information](#)