ADMINISTRATIVE PROCEDURE

Business Administration	Records Management and Retention	BUS #08

Revised: **June 2026**

Background

The division's records are subject to applicable access and privacy legislation, including the Access to Information Act (ATIA) and the Protection of Privacy Act (POPA), and must be managed throughout their lifecycle (creation, storage, retention, access, and disposition) in a consistent and secure manner.

Christ The Redeemer (CTR) Catholic Schools makes information available to the public, including financial materials and statements, annual reports, financial budgets and plans and other financial matters, and is responsible for its management, custody and control, whether in electronic or other recorded format. With respect to operating the division in a sound and prudent fiscal manner, the Board's Financial Guidelines Policy delegates to the Superintendent to "ensure that Public Sector Accounting Principles for the public sector are followed".

This AP applies to records in any format, including paper, email, messaging platforms, photos/video, and electronic systems. This procedure supports the division's Privacy Management Program (PMP) and Security Classification standard by establishing lifecycle controls for records, including retention, access, secure storage, and disposition.

Definitions

- **Record:** Recorded information created, received, or maintained in the course of Division business, regardless of format.
- **Official Record:** The authoritative version to which the retention schedule applies.
- **Transitory Record:** Short-term information with no ongoing business value once reference use ends (e.g., duplicates, routine notices, working drafts not needed to document decisions). Transitory records may be securely deleted/destroyed when no longer required for reference, provided no legal hold applies and the record is not required as evidence of a decision or action.

Procedures

1. Information must be protected in accordance with its sensitivity and disclosed only as authorized by law, policy, or an approved business purpose.
2. Records must be handled (stored, shared, transmitted, and disposed of) in accordance with the division's Security Classification standard.
3. Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and records management practices.
4. Each person using CTR Catholic's information is responsible for the management and safekeeping of information under their control by collection, use, disclosure or disposal of information.

5. Official records must be stored in division-approved systems and repositories. Records that document decisions, direction, approvals, student/program delivery, financial transactions, incidents, or legal obligations must not be stored on personal devices or personal accounts (e.g., personal email, personal cloud storage).
6. Security measures must be used for sensitive information, and caution must be used when conveying confidential information. This information must be stored in a secure division-approved location for protection against unauthorized access.
7. Records destruction must be immediately suspended when litigation is anticipated or underway, an audit/investigation is initiated, an access request is received or anticipated, or a privacy incident requires preservation of evidence. Staff must follow "do not destroy" instructions issued by the division.
8. Destruction of records must be secure and appropriate to the record type and sensitivity (e.g., secure shredding for paper; secure deletion for electronic records) and must be documented in a disposition/destruction log in accordance with records management procedures.
9. Records that have met their retention period may be destroyed only in accordance with the Division's approved retention schedule and records management procedures, and only when no legal hold applies.
10. CTR Catholic will maintain an internal schedule regarding the retention and disposition of records. The schedule will include the responsible department, the record, the retention period, the final disposition and reference to the related legislation. The schedule shall not be adjusted without the specific approval of the superintendent responsible for that record, in consultation with the Access and Privacy Coordinator where appropriate.