BYLAW 2025-12

A BYLAW OF THE MUNICIPAL DISTRICT OF LESSER SLAVE RIVER NO. 124 IN THE PROVINCE OF ALBERTA, FOR THE PURPOSE OF PROVIDING REGULATIONS AND PROCEDURES FOR THE RETENTION AND DISPOSAL OF RECORDS

WHEREAS, Section 214(2) of the Municipal Government Act, Chapter M-26.1, R.S.A. 1994, and amendments thereto, provides that a Council may pass a bylaw respecting the destruction of records and documents of the municipality;

AND WHEREAS, the Council of the Municipal District of Lesser Slave River No. 124 wishes to establish a comprehensive framework for the retention, digitization, classification, and disposition of municipal records in compliance with applicable legislation, standards, and best practices. Inclusive of correspondence, records, receipts, vouchers, instruments, notes, and other papers or alternative media records;

NOW THEREFORE, the Council of Municipal District of Lesser Slave River No. 124 in the Province of Alberta, duly assembled, enacts the following:

1. This Bylaw is enacted under the authority of:
    a. Section 214 of the Municipal Government Act (MGA)
    b. Access to Information Act (ATIA) and Protection of Privacy Act (POPA)
    c. ISO 13008:2022 – Digital Records Conversion and Migration
    d. Alberta Municipal Affairs Guidelines
2. That the following definitions shall apply in respect of this bylaw:
    a. **Chief Administrative Officer (CAO):** The CAO is the senior municipal official responsible for oversight, approval, and enforcement of all record retention, destruction, and compliance activities.
    b. **Record Officer:** The designated municipal staff member responsible for managing the lifecycle of municipal records, including classification, retention, secure destruction, certification, compliance, and audit.
    c. **IT Security Officer:** The designated municipal staff member responsible for secure digital record management, including data sanitization, audit trails, certificate validation, and cybersecurity protocols.
    d. **Administration:** Municipal staff responsible for supporting record management activities, including filing, indexing, and witnessing destruction events.
    e. **Records:** All correspondences, ledgers, receipts, vouchers, instruments, maps, rolls, notes, or other documents, records, papers, or electronic records held by the Municipal District of Lesser Slave River No.124 in any form.
    f. **Digitization:** The process of converting physical records to digital format in accordance with ISO 13008:2022.
    g. **Disposition:** Final action taken on a record (destroy, archive, transfer).
    h. **Transitory Record:** Records with short-term or no administrative, legal, fiscal, or historical value.
    i. **Substantive Record:** Records with enduring value requiring retention.

3. Symbols
    a. That when used in this bylaw and Schedule attached hereto, and in the operation of any records management systems of the Municipal District of Lesser Slave River, symbols shall be used to designate the form of retention or disposal as follows:

D	Destroy	NLN	No Longer Needed
P	Permanent	DOE	Date of Execution
R	Review	SAP	Same as Paper
LOA	Life of Asset	S/O	Superseded/Obsolete

Note: All records previously labeled with the disposition code D (Do Not Destroy) shall be grandfathered under the new disposition code P (Permanent).

4. Retention, Disposition and Schedule Adoption
    a. The Chief Administrative Officer (CAO) and/or the Record Officer is authorized to retain municipal records beyond their scheduled disposition period where litigation, investigation, or other legal proceedings are reasonably anticipated. Such decisions must be documented in the retention index and flagged within the municipality's digital records management system by the IT Security Officer.
    b. In accordance with the Access to Information Act (ATIA), all records that inform decisions affecting individuals must be retained for a minimum period of one (1) year from the date of final action or decision.
    c. Records designated for destruction must be disposed of in accordance with approved procedures. No duplicate or residual copies shall be retained following authorized destruction.
    d. Records classified as Permanent (P) must be preserved indefinitely, except where the original record has been digitized and stored in a compliant system that meets the standards set forth in ISO 13008:2022 and applicable legislation.
    e. Schedule 'A' is hereby adopted as the official retention and destruction schedule of the Municipal District and shall govern the classification, retention period, and disposition method for all municipal records.
    f. All municipal records must be retained or disposed of strictly in accordance with the provisions outlined in Schedule 'A, subject to any applicable legislative or regulatory requirements.

5. Destruction Procedures and Certification
    a. The destruction of municipal records must be conducted in a secure and documented manner, in accordance with applicable legislation and approved procedures.
    b. The Record Officer shall issue a written certification for each destruction event, referencing the applicable retention schedule and item. This certification must confirm that the destruction was authorized, complete, and compliant with the municipality's records management policies and legal obligations.
    c. The IT Security Officer shall validate the destruction of digital records by confirming the use of secure and verifiable methods, including but not limited to cryptographic erasure, overwriting, or degaussing. The Officer shall also maintain tamper-proof audit logs documenting all destruction activities, in accordance with the standards prescribed under the Access to Information Act (ATIA), the Protection of Privacy Act (POPA), and ISO 13008:2022.
    d. All destruction events must be observed and attested to by a municipal staff member who is not directly involved in the destruction process. A written attestation shall be completed and permanently preserved, detailing the date, time, method of destruction, personnel involved, and reference to the applicable retention schedule.

6. Index and Inventory
    a. The Record Officer shall maintain a permanent and centralized index of all municipal records that have been lawfully destroyed. This index must include comprehensive metadata for each record, including the record title, classification code, format (physical or digital), date and method of destruction, personnel involved, and reference to the applicable retention schedule as outlined in Schedule 'A'.
    b. A centralized inventory of all active and archived municipal records shall be maintained and updated on a regular basis. This inventory shall enable all departments to accurately track the status, location, and disposition of records, thereby reducing duplication, enhancing accessibility, and supporting operational continuity in accordance with the Access to Information Act (ATIA) and the Protection of Privacy Act (POPA).
    c. The IT Security Officer shall maintain secure, tamper-proof audit trails documenting all actions performed on digital records, including access, modification, and deletion. These audit logs must be backed up in accordance with approved retention protocols and preserved for the duration specified in the applicable retention schedule. All audit trail procedures must comply with Access to Information Act (ATIA) and the Protection of Privacy Act (POPA), and ISO 13008:2022 standards governing digital record integrity and lifecycle management.

7. Security and Storage
    a. The Chief Administrative Officer (CAO) shall exercise oversight over the municipality's records storage framework, ensuring that all systems and procedures uphold the principles of integrity, confidentiality, and statutory compliance.
    b. The Record Officer shall be responsible for the secure storage of physical records. This includes implementing appropriate environmental controls, access restrictions, and classification protocols to safeguard records against unauthorized access, deterioration, or loss.
    c. The IT Security Officer shall ensure the secure storage of digital records by applying encryption standards, access control mechanisms, and routine backup procedures. All digital storage practices must comply with the requirements set forth in the Access to Information Act (ATIA), the Protection of Privacy Act (POPA), and ISO 13008:2022, ensuring the long-term preservation, integrity, and recoverability of electronic records.

8. Digitization and Physical Record Destruction
    a. Physical records may be eligible for destruction following digitization, provided that the following conditions are met:
        i. The digital reproductions conform to the standards set forth in ISO 13008:2022 – Digital Records Conversion and Migration.
        ii. All associated metadata and audit trails are preserved to ensure authenticity, reliability, and traceability.
        iii. A Destruction Certificate is duly executed and permanently retained in the municipal records system.
    b. The Chief Administrative Officer (CAO) shall approve the destruction process as the senior authority responsible for oversight of the municipality's records management program. Such approval shall ensure strategic accountability and confirm that all destruction decisions are consistent with applicable legal, operational, and governance standards.
    c. The IT Security Officer shall validate digital compliance by confirming that digital records are destroyed using secure and verifiable methods, including but not limited to overwriting, cryptographic erasure, or degaussing. This validation must align with ISO 13008:2022, which prescribes procedures for maintaining the integrity and usability of digital records throughout their lifecycle. Validation shall include confirmation that metadata and audit trails remain intact and that the digital destruction is irreversible.
    d. The CAO approves the process as the senior authority responsible for oversight of the municipality's records management program. This approval provides strategic accountability and ensures that destruction decisions are aligned with legal, operational, and governance standards.

9. Year-End Filing and Flow of Information
    a. The Record Officer shall exercise oversight over the indexing of municipal records. The IT Security Officer shall be responsible for ensuring the integrity, security, and operational continuity of all digital recordkeeping systems.
    b. Each municipal department is required to complete the Year-End Filing Template, index all applicable records, convert physical records to digital format where appropriate, and upload finalized records to the designated electronic records management system (Laserfiche), in accordance with approved retention schedules.
    c. Draft and work-in-progress documents shall be managed within the SharePoint platform, utilizing version control protocols to ensure accurate tracking of revisions and compliance with internal documentation standards.
    d. Finalized records shall be securely stored in Laserfiche, accompanied by complete metadata and retention classifications, in accordance with the Access to Information Act (ATIA), the Protection of Privacy Act (POPA), and ISO 13008:2022 standards for digital records conversion and lifecycle management.

10. Email, Digital and Hard Copy Management
    a. All email communications shall be classified in accordance with their administrative, legal, fiscal, or historical value, as follows:
        i. Transitory Records: Emails deemed to have no enduring value shall be securely deleted once their immediate purpose has been fulfilled.
        ii. Substantive Records: Emails containing information of lasting significance shall be retained in accordance with the applicable retention schedule and classified accordingly.
    b. Email records shall be archived in a manner that ensures they are fully searchable, retrievable, and compliant with metadata and indexing standards prescribed under the Access to Information Act (ATIA) and the Protection of Privacy Act (POPA).
    c. Physical records shall be indexed using standardized classification codes, securely stored in designated municipal facilities, and subject to annual review to confirm retention status and compliance with approved schedules.

11. Secured On-Site and Digital Destruction
    a. Physical records that have been approved for destruction shall be disposed of securely on municipal premises using one or more of the following authorized methods:
        i. Cross-cut shredding equipment that meets provincial privacy and security standards;
        ii. Incineration, where permitted by applicable environmental and municipal regulations;
        iii. Contracted mobile shredding services that are certified to handle confidential municipal records in accordance with legislative requirements.
    b. Digital records approved for destruction shall be securely deleted using industry-recognized data sanitization methods, including:
        i. Overwriting of data using multiple-pass algorithms;
        ii. Cryptographic erasure, rendering data irretrievable through key destruction;
        iii. Degaussing, where applicable, to eliminate magnetic storage traces.
    c. Only designated municipal personnel authorized by the Chief Administrative Officer (CAO) may conduct or supervise destruction activities. All destruction events must be witnessed by a staff member who is not directly involved in the process. A Destruction Certificate shall be completed for each event, documenting the date, time, location, method of destruction, personnel involved, and reference to the applicable retention schedule. This certificate shall be permanently preserved in the municipality's official records system in accordance with the Access to Information Act (ATIA), the Protection of Privacy Act (POPA), and ISO 13008:2022 standards.

12. Compliance, Audit, and Enforcement
    a. The municipality shall conduct annual audits to verify compliance with approved retention schedules, destruction protocols, metadata standards, and accessibility requirements. These audits must be documented and reviewed in accordance with applicable legislation, including the Access to Information Act (ATIA) and the Protection of Privacy Act (POPA).
    b. The Record Officer shall be responsible for executing the audit process, including the review of physical and procedural compliance. The IT Security Officer shall verify digital compliance, ensuring that electronic records management systems meet statutory and technical standards for integrity, security, and traceability.
    c. Any instance of non-compliance with this bylaw or associated policy or procedures may result in disciplinary action, subject to the municipality's internal governance policies. All violations shall be formally reported to Council by the Record Officer, accompanied by supporting documentation and recommended corrective measures.

Should any provisions of this Bylaw be declared invalid, the invalid shall be severed, and the remaining provisions of this Bylaw shall be maintained.

BYLAW 2025-12

Bylaw 2001-01 and the attached schedules are hereby rescinded.

This Bylaw takes effect immediately on **10th of September 2025.**

READ a first time this 10th day of September 2025

READ a second time this 10th day of September 2025

APPROVED UNANIMOUSLY this 10th day of September 2025

READ a third and final time this 10th day of September 2025

_"Original Signed"_____

Murray Kerik, Reeve

_"Original Signed"_____

Barry Kolenosky, Chief Administrative Officer