Town of Bon Accord
building for tomorrow

Policy 26-156

DATA CLASSIFICATION

SECTION: Administration / Council
DEPARTMENT: Administration / Public Works / Finance / Community Services
COUNCIL APPROVAL DATE: July 7, 2026
LAST REVIEWED BY COUNCIL: July 7, 2026

POLICY STATEMENT

In accordance with the Privacy Management Program Policy and procedures, the Town is committed to ensuring that records under the Town's custody and control are handled with due care and that their classification reflects the level of sensitivity each document requires, including records containing personal information.

PURPOSE

To establish standards for classifying and securely storing Town records, ensuring appropriate protection is aligned with sensitivity, risk, and legal requirements.

SCOPE

This policy applies to all data and information assets created, received, stored, Processed, or transmitted by employees, contractors, and partners of the Town.

DEFINITIONS

"Councillors" means the elected officials of the Town of Bon Accord.

"Employee" means Town employees, and any person who performs a service for the Town as an appointee, volunteer, student, or under a contract or agency relationship with the Town.

"Privacy Legislation" means collectively: the Access to Information Act, Access to Information Act Regulation, Protection of Privacy Act, Protection of Privacy (Ministerial) Regulation, and Protection of Privacy Regulation, as amended from time to time.

"Privacy Management Program" means the Town's documented policies and procedures that promote its compliance with its duties under Privacy Legislation, as outlined in the Town's Privacy Management Program Procedures.

RESPONSIBILITIES

I. Roles and Responsibilities

1. **Employees and Councillors must:**
   - **a.** Determine appropriate classification levels and ensure data is stored and handled in accordance with the classification levels outlined in this policy.
   - **b.** Understand and apply required security and storage controls for the classification of data they handle.
   - **c.** Notify the Privacy Officer if the security classification of personal information has changed so that the Personal Information Bank procedure may be updated.
2. **Third Party IT must:**
   - **a.** Implement and maintain technical storage controls including encryption, access management, backup, and recovery.
3. **Privacy Officer must:**
   - **a.** Ensure compliance with privacy legislation and oversee classification adherence for personal and sensitive information.
   - **b.** Monitor how classifications are used by Employees and Councillors to assess risk of security breaches.
   - **c.** Request information from the Town's IT provider twice annually to ascertain that backups, data encryption and other security measures are in compliance with this policy.

II. Classification

1. Classification of documents and information does not require manual labelling.
2. Employees and Councillors are responsible for assessing the appropriate classification level based on the content of individual documents and the context

for which it is being used.

3. A classification level may change as the context in which it exists changes. For example, a closed session policy may be confidential during Council discussions but may be released to the public once the policy is approved for public viewing.
4. Access to files containing personal information, as defined in Privacy Legislation, is limited to the department, Employee or Councillor as outlined in the Town's Personal Information Bank procedure.

III. Compliance and Review

1. Regular reviews of classification and storage requirements are to be completed in conjunction with review of the Privacy Information Bank Policy and Procedures.
2. Non-compliance may result in disciplinary or legal consequences.

IV. Classification Levels

1. Examples described in the chart below are not an exhaustive list.

Classification Level	Description	Examples	Security Requirements	Storage Requirements
Public	Information intended for public disclosure with no adverse impact.	Bylaws, public policies, agenda packages (excluding closed session), public meeting minutes.	Basic administrative controls. Store in access-controlled internal systems or rooms. Hard copies of permanent documents stored in a secure environment to ensure safe handling. Freely accessible and shareable.	Storage environment does not require special controls except hard copies of permanent records such as bylaws and minutes which will be kept in the vault. Can be stored on general IT infrastructure or public-access systems. Proactively shared on the Town website where appropriate.
Internal Use Only	Information intended for internal use with minimal risk if disclosed.	Internal policies, memos, third party contacts.	Basic administrative controls. Store in access-controlled internal systems or rooms. Access limited to internal personnel.	Stored in environments with basic physical access controls (e.g., locked cabinets). Secure handling and destruction recommended.
Protected	Information that could cause harm if compromised.	Personal contact info, third party contracts, operational data, financial information	Access restricted to authorized users. Administrative and physical controls in place. Encryption and back ups required.	Stored in secure, access-controlled rooms or internal systems. Secure destruction of records required.
Restricted	Information that could cause extreme harm if compromised.	Closed session records, law enforcement data, HR and employee files, WCB claims.	Strict access restrictions. Data must be encrypted. Backup and recovery with secure offsite storage.	Stored in limited access areas in accordance with the Town's PIB Policy and Procedures. Only shared with authorized individuals on as needed basis. Secure destruction of records required.

V. Related Documents

- Privacy Management Program Policy and Procedures
- Personal Information Bank Policy and Procedures
- Records Retention and Disposition Bylaw