CODE: CN.AR

TOPIC: Creation, Use and Maintenance of Division Information

EFFECTIVE DATE: (29-01-2020)

ISSUE DATE: (29-01-2020)

REVIEW YEAR: (2024)

OBJECTIVE

Edmonton Public Schools believes in managing information as a strategic Division resource and to this end is guided by provincial legislation and international record standards.

DEFINITIONS

Records means a piece of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

Significant Records, regardless of physical form, created or received by the Board or an agent of the Board, are those which document:

a. results of significant daily activities that support the mission and objectives of the Division;
b. advice and recommendations made to management and the decisions and the rationale for those decisions and actions taken or not taken as a result, along with supporting documentation;
c. problems encountered in business operations and the steps taken to resolve the problems;
d. interactions with the public, students, parents, stakeholders, consultants, vendors, business partners, and other school jurisdictions; verbal communications such as meetings, telephone calls and face-to-face discussions where significant actions or decisions have occurred;
e. legal agreements of any kind, including contracts, along with supporting documentation;
f. policy, business planning, performance measurement and budget activities, with supporting documentation;
g. work done for the Division by consultants and other external resources; and actions and decisions where payments are made or received, funds committed, services delivered or obligations incurred.
h. the history of the Division; the changes in its organization, departments, staff and programs; facilities and sites; policies, procedures; and relationships with external agencies, including printed documents; provincial government documents which affect the operation of Edmonton Public Schools; curriculum material, and individual school records such as yearbooks and photographs.

Essential Records are those records which an organization requires to operate, records which must be retrievable after a disaster using the Disaster Recovery Plan. (see A.8)

Transitory Records are those which have no enduring value to the Division, no legal requirement for retention and have fulfilled their purpose. Types of transitory records include:

a. a duplicate: an exact copy of a document filed in an official file system;
b. a document without any enduring value: information useful only for a brief period of time;
c. advertising materials: anything that offers a product or service for the Division to purchase;

d. blank information media: materials whose purpose is to hold information (e.g., blank forms, blank compact disks)
e. draft documents and working materials; preliminary versions of intermediate documents, calculations and notes used in the preparation of final versions; and
f. external publications: books, magazines, pamphlets, software documentation.

Life Cycle of a Record

a. Active Records - records that are used on a frequent basis and for which the action, service, transaction, project is not complete. These records are stored on site and access to them is immediate.
b. Semi-Active Records - records for which the action, service, transaction or project is complete and which are required to be accessible for follow up, evaluation, audit, or legal requirements during a possible dispute. These records are not immediately accessible and may be stored at a centralized Division records storage facility.
c. Closed Records - records that have met all organizational and legal requirements. Records at this stage are either destroyed or transferred to the custody and control of Archives and Museum.

Personal Information

a. Under the *Freedom of Information and Protection of Privacy Act*, "personal information" means recorded information about an identifiable individual, including:
b. the individual's name, home or business address or home or business telephone number,
c. the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
d. the individual's age, sex, marital status or family status,
e. an identifying number, symbol or other particular assigned to the individual,
f. the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
g. information about the individual's health and health care history, including information about a physical or mental disability,
h. information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given, anyone else's opinions about the individual, and
i. the individual's personal views or opinions, except if they are about someone else.

Employee includes a person who performs a service for the Division as a staff member, appointee, volunteer or student or under a contract or agency relationship with the Division.

REGULATION

A. DIVISION RECORDS

1. The management of all Division records requires a number of initiatives as are listed in this section. These initiatives will be under the direction of Division Information Management. The Division Information Management program shall be a strategically developed program in which all components must support each other to achieve the goal of effectively managing information assets.

2. Division Technology shall review all significant acquisitions of information management technologies to ensure the existing infrastructure can support the technology and new technologies fit within the overall architecture of the Division for software that affects multiple users and/or department-level applications. Division Technology shall review how technology may affect the Division's compliance with

external requirements (e.g., the *Freedom of Information and Protection of Privacy Act*) in consultation with Division Information Management.

3. Consistent Classification Scheme
   A consistent methodology for organizing records called a classification scheme shall be developed and maintained by Division Information Management in collaboration with decision units. Decision unit administrators shall ensure the implementation of the Division classification scheme. All staff will file significant records according to the classification scheme.

4. Records Retention Schedule
   a. Division Information Management shall ensure the retention periods for records:
      i. meet legislated requirements;
      ii. support business operations and educational decisions;
      iii. provide evidence of educational programs, business transactions or the history of the Division;
      iv. facilitate service delivery; and
      v. support the Division's ability to respond to ongoing litigation.
   b. The records retention schedule shall document:
      i. criteria to determine when a record can be closed;
      ii. concurrent activities that may override the retention schedule, such as litigation or a historically significant event;
      iii. specific storage requirements and migration strategies to facilitate long term retrieval of information;
      iv. identification of essential records and the applicable recovery practices;
      v. those records which will have archival or research value;
      vi. those records which contain personally identifiable information;
      vii. the length of time records must be stored on-site and off-site;
      viii. opinions from legal, technology, Division Information Management, and finance;
      ix. security procedures; and
      x. disposal instructions.
   c. The records retention schedule shall be approved by the Superintendent of Schools.

5. Responsibility for Records
   Central service decision unit administrators and principals, in their role as Record Managers and FOIP Coordinators, shall implement the retention schedule by:
   a. maintaining the continuity of records essential to the conduct of business in their area of responsibility;
   b. controlling access to all Division records in their area of responsibility;
   c. maintaining an inventory of the Division records in their area of responsibility;
   d. arranging for the safe storage of the Division's records in their area of responsibility, for the period of time prescribed in Division records retention schedule;
   e. consulting with Legal Counsel, Division Information Management or Archives and Museums regarding exceptions to the retention schedule; and
   f. employing appropriate transfer and disposal procedures.

6. Access Provisions for Semi-Active and Archival Records
   a. Records that are semi-active may be stored in a centralized Division records storage facility. Central service decision unit administrators and principals remain responsible for the records until final

disposition. Records that are in storage shall be available for reference with the authorization of the responsible decision unit administrator or the Supervisor of Division Information Management. Retrieval services shall be provided to staff.

b. Division Information Management shall be responsible for the management of centralized records storage facility.
c. Archives and Museum shall be responsible for the management of Division archives.
d. Archives and Museum may grant access to records containing personal information if:
    i. the research proposal meets Division criteria for acceptable research practices in accordance with IQ.AR - Conducting Research Within the Division
    ii. the research proposal is of educational benefit or significance to the Division; and
    iii. the disclosure otherwise conforms to the requirements of Section 42 of the *Freedom of Information and Protection of Privacy Act.*

7. Forms Management
   Decision unit administrators and principals shall be responsible to ensure all forms collecting personal information meet published Division standards. A central repository for all Division form templates shall be maintained by Division Information Management. Communications and Division Information Management shall jointly develop and publish standards for content and appearance of all Division forms. The Division FOIP Coordinator will offer advice and assistance on appropriate collection of personal information.

8. Disaster Recovery
   Division Information Management shall be responsible for the development and maintenance of a methodology for defining, identifying, and protecting essential records. Decision unit administrators and custodial business units shall be responsible for ensuring protective measures are in place.

9. Information Security
   a. Division Information Management shall develop and maintain a consistent set of categories for the classification of information based on sensitivities and disclosure risks. Categories shall specify criteria and appropriate security measures to protect the information.
   b. FOIP Coordinators shall ensure that security arrangements are in place for information under their custody and control in keeping with Division standards.
   c. Division Technology shall provide advice and assistance to principals and decision unit administrators with respect to appropriate electronic security measures.

10. Management of Contracts
    When a principal or decision unit administrator enters into a contract agreement with another individual or organization, they are placing obligations on the Division. A contract is defined as any legally binding agreement, written or verbal, between the Division and another individual or organization. Purchasing and Contract Services provides assistance regarding vendor contracts in accordance with CWA.AR - Expenditure of Public Funds. General Counsel shall create and maintain a standards document to assist principals and decision unit administrators in protecting Division interests for other contracts. Before entering into negotiations that will result in a contract, principals and decision unit administrators should consult the standards document. Contracts obligating the Division to release or exchange personal information shall meet Division standards.

B. COLLECTING, RECEIVING AND CREATING PERSONALLY IDENTIFIABLE INFORMATION

1. Collection of Personal Information
    a. Personal information shall be collected only if it relates directly toward and is necessary for an operating program or activity of the Division and the Division has the authority to collect the information.

2. Processes for Collection of Information
    a. Employees must take appropriate steps to ensure personal information is accurate. When collecting personal information staff shall inform the individual as to why the information is being collected, how long the information will be retained and who they can contact for clarification.
    b. Programs and practices to ensure the Division meets its legislated requirements shall be developed and implemented as defined in this section.

3. Protection of Privacy
    a. All personally identifiable information shall be managed to ensure individual privacy is maintained. Division Information Management shall develop and publish standards and best practices. Decision unit administrators shall be responsible to meet the prescribed guidelines and standards for all personally identifiable information in their area of responsibility.
    b. All personally identifiable information shall be collected and disclosed on the basis of delivering a service or program. All staff information sharing shall be limited to only what is needed in order to complete a task. All personal information is sensitive; therefore privacy shall be protected during the collection, storage, use, sharing and transmission of personally identifiable information by all staff.

C. ACCESS TO INFORMATION

The right of access is the cornerstone of openness and accountability of public bodies. The *Freedom of Information and Protection of Privacy Act* is in addition to and does not replace existing procedures for the public to obtain access to information from the Division. A request for information under the *Freedom of Information and Protection of Privacy Act* is a costly undertaking for the Division and wherever possible, requests for information should be accommodated outside of the *Freedom of Information and Protection of Privacy Act*, but in keeping with the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*.

1. Right of Access
    a. The public has the right of access to records held by public bodies, subject to narrow and specific exceptions.
    b. An individual's right of access to their own information is significant and any exceptions to access should be interpreted with a view to giving an individual as much access as possible to their own personal information.
    c. Any disclosure of personal information must be in compliance with the privacy provisions of the *Freedom of Information and Protection of Privacy Act*.

2. FOIP Requests
    a. A request for information under the *Freedom of Information and Protection of Privacy Act* must be made in writing and sent to the attention of the Division FOIP Coordinator. The request may be made by completing a Request to Access Information Form or by writing a letter requesting specific records and referencing the *Freedom of Information and Protection of Privacy Act*.

b. Employees must not reveal the identity of a FOIP applicant in any communication, formal or informal, with any other individual unless the other individual requires the identity to search for responsive records.

3. Fees for processing a FOIP Request
   Edmonton Public Schools is authorized to charge fees for services related to requests under the *Freedom of Information and Protection of Privacy Act*, which fees payable shall be in accordance with and shall not exceed the fees as provided in the *Freedom of Information and Protection of Privacy Regulations*, *Alta. Reg. 186/2008* as amended from time to time, or a successor Regulation that sets fees for request for information.

D. ROLES AND RESPONSIBILITIES

Each employee is responsible for properly handling and protecting information in their custody and control. Descriptions of various roles throughout the organization are detailed below; each employee will find themselves described in one or more of the roles.

1. The Superintendent of Schools is designated as the FOIP Head of Edmonton Public Schools for the purposes of the *Freedom of Information and Protection of Privacy Act*.

2. The Division FOIP Coordinator shall be responsible for:
   a. providing advice and assistance to employees in understanding and applying the legislated requirements related to access of information and protection of privacy
   b. providing training programs on access to information and protection of privacy and coordinating participation in FOIP courses offered by the Government of Alberta
   c. advising staff on information that can be released as a routine disclosure or only under a FOIP request
   d. managing the FOIP request process for the Division
      i. assisting applicants
      ii. assigning requests
      iii. monitoring and tracking the processing of requests
      iv. meeting time limits and notification requirements
      v. considering representations from third parties
      vi. calculating fee estimates and collecting fees
   e. setting up practices and procedures to ensure that privacy protection measures are implemented and carried out
   f. coordinating any negotiations, mediations, inquiries, investigations, and audits with the Office of the Information and Privacy Commissioner (OIPC)
   g. ensuring staff are aware of other Acts and regulations that restrict the disclosure of information
   h. coordinating the development and maintenance of a directory of records and establishing a list of Personal Information Banks
   i. providing training for all staff for managing and handling information specific to their responsibilities.

3. FOIP Coordinators
   The following positions shall be designated Records and FOIP Coordinators:
   a. Principals
   b. Decision Unit Managers/Administrators

c. Division FOIP Coordinator

4. The Division has two large records collections containing personally identifiable information. Each collection is identified below with a designated FOIP Coordinator.
   a. Student Records - Manager Student Information
   b. Personnel Records - Director Staff Relations.

5. FOIP Coordinators shall be responsible for:
   a. implementing Division policies, regulations, and procedures to manage records under their custody and control;
   b. setting up practices and procedures to ensure that the management and security of records in the custody and control of their decision unit or school meets Division and legislated requirements related to access to information and protection of privacy;
   c. ensuring staff follow appropriate practices and facilitating training opportunities;
   d. identifying and providing access to information that can be released as a routine disclosure or outside of a FOIP Request;
   e. assisting the Division FOIP Coordinator in responding to a FOIP request.

6. All employees shall be responsible for:
   a. documenting, creating and organizing Division information in the course of their work in a way that is objective and professional;
   b. following Division record management procedures and respecting the principles of access to information and protection of personal privacy in an open accountability organization;
   c. protecting all information while in their custody and control, ensuring the risk of unauthorized disclosure of personal or other confidential information is minimized;
   d. making sure they have authority to collect personal information they request;
   e. ensuring personal information is used in a way that is consistent with the original purpose of collection;
   f. sharing personal information only with individuals or organizations that have the right of access or the consent of the individual about whom the information applies;
   g. exercising their judgment in refusing to confirm the existence or nonexistence of a record if it is believed that an applicant's knowledge that a record exists or not may pose a danger to an individual or would be an unreasonable invasion of their privacy;
   h. assisting individuals in accessing information in accordance with Division procedures;
   i. taking reasonable steps to verify accuracy of information used to make decisions affecting individuals.

REFERENCES

CN.BP - Managing Division Information
CWA.AR - Expenditure of Public Funds
IQ.AR - Conducting Research within the Division
Freedom of Information and Protection of Privacy Act
Government of Alberta Freedom of Information and Protection of Privacy Website
Request to Access Information Form