SECTION 5

RECORDS AND INFORMATION MANAGEMENT

5.04 UNSOLICITED PERSONAL INFORMATION

AUTHORITY: *ARCHIVES AND RECORDS ACT*
FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

ADMINISTRATION: DEPARTMENT OF EDUCATION AND EARLY YEARS
PUBLIC ARCHIVES AND RECORDS OFFICE
DEPARTMENT OF JUSTICE AND PUBLIC SAFETY
ACCESS AND PRIVACY SERVICES OFFICE

EFFECTIVE DATE: DECEMBER 2023

5.04 UNSOLICITED PERSONAL INFORMATION

(1) PURPOSE

This policy establishes the proper treatment of personal information in the possession of a public body that the public body is not authorized to collect under section 31 of the *Freedom of Information and Protection of Privacy Act* (FOIPP).

(2) BACKGROUND

Section 31 of FOIPP stipulates the authorized purposes under which a public body may collect personal information. Section 32 of FOIPP requires a public body to collect personal information directly from the individual the information is about except in certain circumstances.

Occasionally, individuals voluntarily send records to a public body containing their personal information or personal information of a third party that the public body has not requested. A public body might mistakenly receive records (e.g., faxes, emails) containing personal information intended for another recipient. If the public body is not authorized to collect personal information obtained in either scenario, it cannot retain it. However, destroying, severing, or returning the record should also comply with the *Archives and Records Act* (ARA).

Personal information obtained under any of the circumstances described above may form part of a public record. Destroying or severing such personal information may alter or destroy public records which are of historic value, and which could be made freely available to the public after FOIPP time restrictions have elapsed. Subsection 19(2) of the ARA stipulates that public records may only be destroyed in accordance with approved records retention and disposition schedules (RDS), which take into consideration the historic value of records. Therefore, public bodies must dispose of such personal information in accordance with the existing RDS for public records or create new schedules to address each scenario.

This policy provides for the return, destruction, or severing of records containing personal information that was unsolicited or mistakenly received by the public body, but that the public body is not authorized to collect, thus allowing public bodies to comply with both the ARA and FOIPP.

(3) APPLICATION

This policy is applicable to all public bodies defined as such in Section 4(c) of this policy. All employees of public bodies, including Executive Council officials, must adhere to this policy.

While this policy **does not apply** to the Legislative Assembly, its committees and offices, or court records or judicial administrative records, **the spirit and intent** of this policy should serve as a guideline for these entities in developing their own policies.

(4) DEFINITIONS

For the purpose of this policy and its accompanying procedures, the following definitions will apply:

(a) **"Final disposition"** is the final stage in the lifecycle of records. It refers to actions taken with regard to public records that are no longer needed for current Government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure. Disposition includes both destruction and transfer of records of historic value to the control and custody of the Public Archives and Records Office.

(b) **"Personal information"** refers to any personal information as defined in clause 1(i) of FOIPP. Section 31 of FOIPP states that no personal information may be collected by or for a public body unless:

(i) the collection of that information is expressly authorized by or under an enactment of Prince Edward Island or Canada;
(ii) that information is collected for the purposes of law enforcement; or
(iii) that information relates directly to and is necessary for an operating program or activity of the public body.

(c) **"Public body"**, means a body as defined by clause 1(1)(f) of the *Archives and Records Act.*

(d) **"Public records"** are records created, received, or maintained by a public body in the course of its activities, including court administration records. Public records can be in physical forms such as printed documents, photographs and maps, or stored as electronic media, such as emails, information stored in databases, word-processing documents and spreadsheets.

(e) **"Record"** means a record of information in any form, including electronic form, but does not include a mechanism or system for generating, sending, receiving, storing or otherwise processing information.

(5) POLICY

Personal information in the possession of a public body that the public body is not authorized to collect must be returned, severed or destroyed in accordance with an approved records retention and disposition schedule. This personal information must not be used in any way in the conduct of Government business.

(6) PROCEDURE

Public bodies sometimes obtain information that was unsolicited or mistakenly received. In such circumstances, the public body should consider the following (*Contact your Records and Information Management (RIM) Coordinator for clarification on these procedures, if needed*):

STEP 1: ASSESS WHETHER THE PUBLIC BODY IS AUTHORIZED TO COLLECT THE PERSONAL INFORMATION

A public body must decide within a reasonable period of time after receiving the information whether or not it is authorized to collect the information under section 31 of FOIPP. *(Refer questions to your FOIPP coordinator)*

If the public body determines that it is not authorized to collect the personal information, then proceed to Step 2.

If the public body determines that it is authorized to collect the personal information, then it may use and disclose the personal information in accordance with FOIPP and retain and dispose of the records in accordance with the *Archives and Records Act* and Records Retention and Disposition Schedules. Steps 2 - 5 are not applicable.

STEP 2: ISOLATE AND PROTECT THE PERSONAL INFORMATION THE PUBLIC BODY IS NOT AUTHORIZED TO COLLECT

If the personal information is not part of a public record, proceed to Step 3 (e.g., a faxed medical report which was meant to be sent to a physician's office, and not to a public body, is not a public record).

If the personal information is part of a public record, the personal information in the public record must:

- be kept in a secure location such as a locked filing cabinet or in a password protected electronic folder and may not be copied or distributed;
- not be used in any way in the conduct of Government business; and
- be managed in accordance with approved Records Retention and Disposition Schedules.

STEP 3: CONTACT THE SENDER TO ADVISE THAT THE PUBLIC BODY IS NOT AUTHORIZED TO COLLECT THE PERSONAL INFORMATION

If the record is not a public record:

- offer to either securely return or securely destroy the personal information. Proceed to Step 5.

If the personal information is part of a public record:

- invite the sender to resubmit the record without the personal information; advise that the public body will securely destroy or return their first sent copy on receipt of a resubmitted record without the personal information at issue; or
- offer to sever the personal or identifying information from the record. Proceed to Step 4.

If the sender cannot be located, does not respond, or does not agree to the public body returning, or severing the record, then:

- if the record is not a public record, the information must be immediately and securely destroyed. Signoffs are not required. It is recommended that the public body document the specifics of the incident including steps taken to contact the sender and return or destroy the personal information.
- where the personal information is part of a public record refer to an approved Records Retention and Disposition Schedule at Steps 4 and 5.

STEP 4: DESTROY OR SEVER ACCORDING TO AN APPROVED RECORDS RETENTION AND DISPOSITION SCHEDULE

Contact the departmental RIM Coordinator to determine which approved Records Retention and Disposition Schedule should be used. If there is no existing retention schedule, then the public body must create one and submit it for approval to the Public Records Committee.

Ensure that the records are kept in a secure location such as a locked filing cabinet or in a password protected electronic folder until they reach their final disposition.

The personal information must not be used in any way in the conduct of Government business.

STEP 5: COMPLETE THE *UNSOLICITED PERSONAL INFORMATION FORM*

Complete the Unsolicited Personal Information Form (Attachment 5.04-I), documenting the specifics of the incident including steps taken to contact the sender, return, sever or destroy the personal information, as applicable.

Obtain appropriate signoffs including the employee who received the records, manager or director of section/division, departmental RIM Coordinator, and Senior Records Manager.

File the Unsolicited Personal Information Form according to public body’s standard recordkeeping system.

(7) INTERPRETATION

In cases where an interpretation is required, such should be referred to the Public Archives and Records Office, who will make the interpretation, or refer the matter to the Secretary to Treasury Board to determine if a Treasury Board decision is deemed necessary.