Use of Personal Information Policy

1. About this document

This policy defines the requirements for departments when using personal information, and should be referred to by program managers when establishing new programs.

2. Definitions

"ATIPP Act" is the *Access to Information and Protection of Privacy Act.*

"Individual" is the person the personal information is about, or their authorized representative.

"Personal Information" is as defined in section 3 of the ATIPP Act.

"Purpose" means the purpose for which the information was originally collected by the department or program.

"Use" of personal information includes, but is not limited to, accessing, looking at, processing, reproducing, transmitting, transporting and sharing of personal information collected by the department.

3. Application

This policy applies to any programs or activities to which the *Access to Information and Protection of Privacy Act* applies and the department is listed in GAM 2.1.

4. Authority

This policy is issued under GAM 2.27 and approved by the DM of HPW on March 13, 2017.

5. Policy

General

- Departments must limit the use of personal information to the minimum amount necessary to accomplish the purpose for which it is needed or used.

- Departments must limit the use of personal information to those employees who need to know the information to carry out the purpose for which the information was collected.
- Employees within the department must not access their own personal information, or the personal information of family, friends or other individuals, unless specifically required as a part of their job duties.
- Personal information may only be used for the purpose for which it was collected and must not be used for any other purpose unless:
    - The other purpose is consistent with the purpose for which it was collected. A new use is deemed to be consistent when:
        - A person would reasonably anticipate or expect the personal information to be used in the newly proposed way.
        - It has a reasonable and direct connection to the original purpose and it is necessary for performing the statutory duties of the department or an authorized program (section 37 of the ATIPP Act).
        - Examples of consistent purpose

          Evaluation of a program

          Departments will have a regular need to evaluate the operation and success of their programs. It would be deemed a consistent purpose to select clients or participants who can participate in that evaluation through questionnaires or interviews.

          Expansion of a program

          Departments set criteria for participation in programs. If the criteria are broadened, individuals who were originally rejected may become eligible. It would be a consistent purpose to use the original submissions to determine eligibility rather than collecting the information again.

    - The individual the personal information is about has consented to the use in accordance with this policy (refer to 'consent' section below).
    - The personal information may be used by departments if the disclosure is in accordance with section 36 to 39 of the ATIPP Act. This information must only be used for the same purpose for which it was disclosed.
        - When determining whether to indirectly collect and use personal information in this manner, consider the following:
            - Is direct collection of the personal information not reasonably feasible?

        - Is the personal information accurate and complete? Will the department take any steps to validate the information?
        - Is information that identifies individuals absolutely necessary to fulfill your purpose? Or can aggregated or de-identified information suffice?
- Departments must update Personal Information Maps when any new collection or use of personal information occurs, if a Personal Information Map was completed previously.

Consent

- Consent for the use of personal information is deemed to be valid when:
    - The individual the information is about has identified or been notified of the information to be used – informed consent.
    - It specifies to whom the personal information may be used and how it may be used beyond the original purpose for which it was collected.
        - This information must be communicated in a manner that can be reasonably understood by the individual.
    - Reasonable steps have been taken to ensure the individual is who they say they are.
    - It is voluntary and not obtained through misrepresentation.
    - The consequences (if any) of refusing to consent have been communicated.
- Written consent is the preferred method and should be signed by the individual.
- Verbal consent is acceptable in instances where written consent is either difficult to obtain or timeliness is an issue.
    - The department must record on the individual's file the contents of the conversation, the date and time of the conversation and who spoke to the individual.
    - When practicable and appropriate, the department will send a letter to the individual confirming the consent.
- An individual who has given consent, may withdraw it by notifying the department. A withdrawal does not have a retroactive effect.
- Departments cannot penalize individuals for refusing to give consent for additional uses by denying them any benefit or service provided in connection with the original collection.

Accuracy

- Before using personal information, departments will take reasonable measures to verify that personal information to be used in a decision-making process is as accurate, up-to-date and complete as possible.

Protecting Personal Information Used

- Departments will limit the use of personal information by administrative, technical and/or physical safeguards[1].
- Departments will adopt appropriate measures to ensure that the use of personal information is monitored and documented in order to permit the timely identification of any unauthorized use or handling of the personal information.

Transmission

- Departments will adopt appropriate safeguards to ensure personal information is protected while it is being transmitted. Such safeguards will be commensurate to the sensitivity of the personal information[2].
    - For example, using the government's approved secure file transfer application.

Retention

- Departments must retain personal information only as long as necessary for the fulfillment of identified purposes, and in keeping with the program's Records Retention and Disposition Schedule as per the *Archives Act*.
- Departments will adopt appropriate safeguards when retaining personal information to protect against accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal. Departments that use personal information to make a decision that directly affects individuals must retain that information for a minimum of one year (section 34 of the ATIPP Act).

[1] For more information on administrative, technical and physical safeguards, see the "Protecting / Safeguarding Information Assets" on the ATIPP office's SharePoint site.
[2] For more information on determining the sensitivity of personal information, see the "Personal Information Classification Guidelines" on the ATIPP office's SharePoint site.