ADMINISTRATIVE PROCEDURE

PROCEDURE NUMBER: J-01
Privacy Impact Assessment (PIA)

1.0 SCOPE OF PROCEDURE

This Procedure is applicable to all Resort Municipality of Whistler (RMOW) staff who are in the planning stages of an update to, or new project or service that collects Personal Information.

2.0 DEFINITIONS

"**Common or Integrated Program or Activity**" means a program or activity that

a. Provides one or more services through
   i. a Public Body and one or more other Pubic Bodies or agencies working collaboratively, or
   ii. one Public Body working on behalf of one of more other Public Bodies or agencies, and
b. is confirmed by regulation as being a Common or Integrated Program or Activity

"**Contact Information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, **business** address, **business** e-mail or **business** fax number of an individual.

"**Data Linking**" means the linking or combining of Personal Information in one database with Personal Information in one or more other databases if the purpose of the linking or combining is different from:

a. the purpose for which the information in each database was originally obtained or compiled; and
b. every purpose that is consistent with each purpose referred to in paragraph a.

"**Data Linking Initiative**" means a new or newly revised system, project, program or activity that has, as a component, Data Linking between

a. two or more Public Bodies, or
b. one or more Public Bodies and one or more agencies.

"**Department Author**" means an RMOW staff member(s) who is drafting the PIA.

"**Information Sharing Agreement**" means an agreement between a public body and one or more of the following:

a. another Public Body
b. a government institution subject to the *Privacy Act* (Canada);
c. an organization subject to the *Personal Information Protection Act* or the *Personal Information Protection and Electronic Documents Act* (Canada);
d. a public body, government institution or institution as defined in applicable provincial legislation having the same effect as this Act;
e. a person or a group of persons;
f. a prescribed entity

that sets conditions on the collection, use of disclosure of Personal Information by the parties to the agreement.

"**Initiative**" means a new or revised system, project, program or activity that may or does contain Personal Information.

"**OIPC**" means Office of the Information and Privacy Commissioner of British Columbia.

"**Personal Information Bank (PIB)**" means means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

"**Personal Information**" means recorded information about an identifiable individual other than **contact information**. Non exhaustive list includes:

- name, e-mail address, phone number, physical address, coded or numerical identifier, credit card number, debit card number, social insurance number, public health card number, signature, photograph of face, IP address, medical information, mortgage information, tax information.

"**Privacy Impact Assessment (PIA)**" means an assessment that is conducted by a Public Body to determine if a current or proposed system, project or activity meets or will meet the requirements of Part 3 of the *Freedom of information and Protection of Privacy Act*.

"**Privacy Risk**" means something that could cause the unauthorized access, collection, use, disclosure, or storage of Personal Information.

"**Public Body**" means

a. a ministry of the government of British Columbia
b. an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2 of the *Freedom of Information and Protection of Privacy Act*, or
c. a local public body; but does not include:
d. the office of a person who is a member or officer of the Legislative Assembly, or
e. the Court of Appeal, Supreme Court or Provincial Court

3.0 PURPOSE

To provide a reference for all local public body (RMOW) staff in regard to their obligation to accurately complete a PIA:

3.1 during the planning stages of the initiative;
3.2 before any agreements, including Information Sharing Agreements, or contracts subject to the initiative are entered into;
3.3 within a time frame that allows for a productive review and any revisions instructed by:
  3.3.1 subject department's management;
  3.3.2 by RMOW Municipal Clerk;
  3.3.3 by RMOW Legislative and Privacy Coordinator;
  3.3.4 by OIPC Analyst.

4.0 AUTHORITY AND REPORTING

4.1 The following RMOW employees are to sign off on a PIA before it is submitted for review to the OIPC:

4.1.2 Subject department(s) management
4.1.3 Subject department(s) General Manager(s)
4.1.4 Municipal Clerk
4.1.5 Legislative and Privacy Coordinator
4.1.6 Manager of IT (when the initiative involves IT elements)

5.0 PROCEDURE

Department Author(s) will:

5.1 Contact the Legislative and Privacy Coordinator during the initial stages of an initiative to let the Legislative and Privacy Coordinator know the scope of the project
  5.1.1 the Legislative and Privacy Coordinator will then determine if a PIA is required and provide resources for the department authors to complete a first draft:
  5.1.1.1 PIA Template – Non Government Ministry Public Bodies (see Appendix A)
5.2 Receive and update any revised draft of the PIA as instructed by the Legislative and Privacy Coordinator

Legislative Services Department

The department will:

5.3 provide department authors with PIA edit instructions;
5.4 submit the final version of the PIA to the OIPC;
5.5 liaise with the OPIC to bring suggested edits back to the department author.

6.0 CONTENT

Under section 69 of the Freedom of Information and Protection of Privacy Act, Public Bodies are directed to include the following elements, where applicable, in any PIA conducted:

6.1 a detailed description of the system, project, program or activity covered by the PIA;

6.2 a list of the elements of information including Personal Information other than Contact Information included in the system, project, program or activity;

6.3 identification of any information including Personal Information involved in the system, project, program or activity that can be accessed from and/ or stored outside Canada;

6.4 identification of whether the system, project, program or activity involves Data Linking and is thus a Data Linking Initiative;

6.5 identification of whether the system, project, program or activity involves a Common or Integrated Program or Activity;

6.6 an information flow diagram and/ or Personal Information flow table that shows how the system, project, program or activity does, or will, collect, use, and/or disclose Personal Information, including the authorities for the collection, use, and disclosure of Personal Information under to the *Freedom of Information and Protection of Privacy Act*.

6.61 an information flow diagram must be included in the system, project, program or activity is related to a Common or Integrated Program of Activity of a Data-Linking Initiative;

6.7 identification of the Privacy Risk within the system, project, program or activity and for each Privacy Risk identified:

6.7.1 an explanation of the likelihood of the Privacy Risk occurring;

6.7.2 an explanation of the degree of impact the Privacy Riske would have on an individual if it occurred; and

6.7.3 a record of the mitigations that have been, or will be, implemented;

6.8 a description of the physical security measures related to the system, project, program or activity;

6.9 a description of the technical security measures related to the system, project, program or activity;

6.10 a description of any specific policies and procedures within the Public Body governing an Employee's management of Personal Information;

6.11 with respect to technical systems, details of access to Personal Information including as applicable, but not limited to:

6.11.1 a description of the permissions government access to the Personal Information;

6.11.2 a description of how access to Personal Information is, or will be, tracked; and

6.11.3 a description of any access controls and/or ways in which unauthorized changes to Personal Information is, or will be, limited or restricted;

6.12 an explanation of how the accuracy of an individual's Personal Information is, or will be, ensured;

6.13 an explanation of how an individual's Personal Information is, or will be, annotated if it is not corrected as per the individual's request;

6.14 with respect to Personal Information, an explanation of the retention and disposition measures that relate to the secure retention and disposition of Personal Information.

6.15 With respect to Personal Information that is used to make a decision that directly affects an individual, an explanation of how any applicable retention and disposition requirements are, or will be met.

6.16 An explanation of any systemic disclosures or regular exchanges of Personal Information included in the system, project, program, or activity;

6.17 for research that is not out of the scope of the *Freedom of Information and Protection of Privacy Act,* as per section 3(1)(e) of that Act, identification of whether the system, project, program or activity does, or will, involve access to Personal Information for research or statistical purposes and references to the research agreement, as required under Section 35 (1)(d) of the *Freedom of Information and Protection of Privacy Act*; and

6.17.1 S. 3(1)(e): This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following: a record containing teaching materials or research information of: (i) a faculty member, as defined in the *College and Institute Act* and the *University Act*, or a post-secondary educational body, (ii) a teaching assistant or research assistant employed at a post-secondary educational body, (iii) other persons teaching or carrying out research at a post-secondary educational body[;]

6.18 identification of whether the system, project, program or activity does, or will, involve a PIB and, where applicable, the PIB summary information under section 69(9) of the Freedom of Information and Protection of Privacy Act for inclusion in RMOW's publically available directory.

Dated this _____day of _____, 2019.

Signed original on file
Alba Banman
Municipal Clerk

Signed original on file
Mike Furey
Chief Administrative Officer

Privacy Impact Assessment for Non-Ministry Public Bodies

[Insert Initiative Title]

PIA#*[assigned by your privacy office(r)]*

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?

Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department/Branch:			
PIA Drafter:			
Email:		Phone:	
Program Manager:			
Email:		Phone:	

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

This section should provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc. For example, the public body may want to overhaul its citizen engagement processes to better align with emerging self-service trends, or a program is moving forward because it is a priority project of the head of the public body.

2. Scope of this PIA

This section should explain, where applicable, exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover. For example, if a public body is overhauling its citizen engagement process to better align with emerging self-service trends and is launching new website features, this particular PIA may only be about the public body's new blog. This blog would then be the "scope" of the PIA. This section may also describe what phase of the initiative this PIA covers.

3. Related Privacy Impact Assessments

This section should identify, where applicable, PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative. To follow on from the above example, this section may cite a PIA that has already been completed on the public body's website or on the video site that the new blog will sometimes link to.

4. Elements of Information or Data

Please list the elements of information or data involved in the initiative. This could include client's name, age, address, work/home email, work/home phone number, educational history, employment history, work status, health information, financial information, photos, comments on a blog, or information specific to your subject area, like stumpage totals, fish license numbers, visitor centre stats, or hiring data.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

Please provide a brief description of whether your information can be accessed from outside Canada, for example, by a service provider that is repairing a system, or if your information is being stored outside Canada, for example, in the "cloud". If your data is stored within Canada and accessible only within Canada, please indicate this.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	yes/no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	yes/no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	yes/no
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	yes/no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes/no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	yes/no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

**** Please note: If your initiative involves a "data-linking initiative" or a "common or integrated program or activity", advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body's privacy office(r) to determine how to proceed with this notification and consultation.***

For future reference, public bodies are required to notify the OIPC of a" data-linking initiative" or a "common or integrated program or activity" in the early stages of developing the initiative, program or activity. Contact your public body's privacy office(r) to determine how to proceed with this notification.

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Please provide a diagram and/or table that shows how your initiative will collect, use, and/or disclose personal information (see examples below). Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. It should also outline the flows of personal information wherever it is transmitted or exchanged.

Privacy Impact Assessment for Non-Ministry Public Bodies

[Insert Initiative Title]

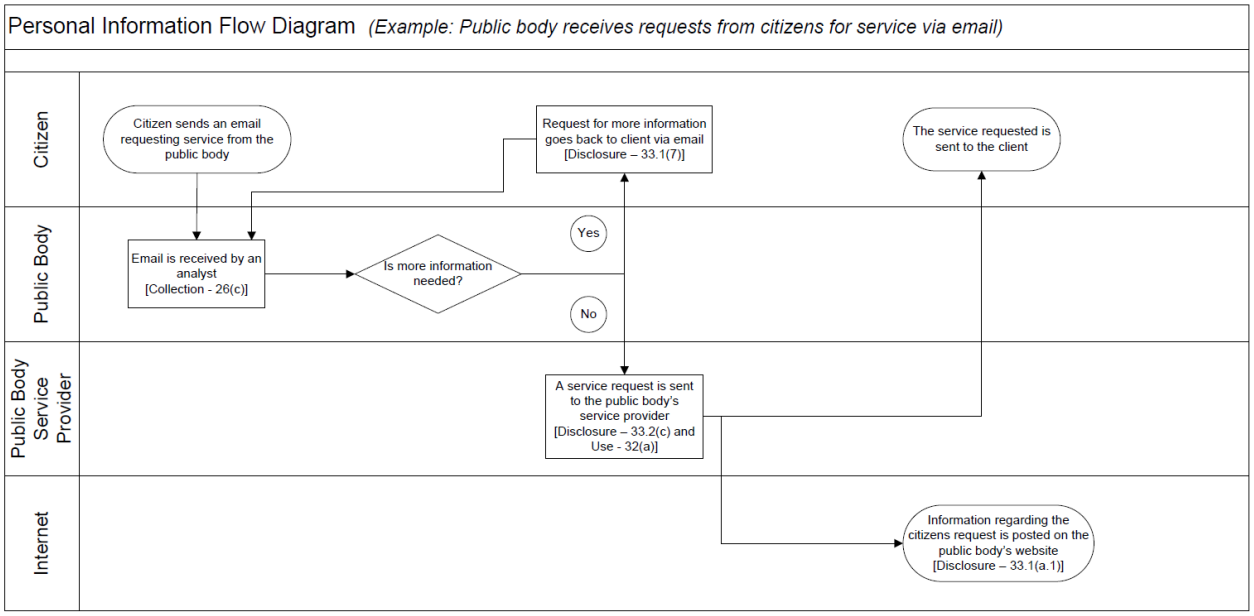
PIA#*[assigned by your privacy office(r)]*

Both a flow diagram and a table must be included if the PIA is related to a common or integrated program or activity or a data-linking initiative.

For ease of reference, the collection, use, and disclosure authorities in FOIPPA can be found in the appendices. If you do not know what the relevant authorities are, please contact your privacy office(r).

Depending on the complexity of your initiative, you may choose to provide one general diagram for the initiative, and more specific diagrams for particular components. If multiple organizations will collect, use, or disclose personal information, the diagram should identify how each organization is involved in the initiative.

Example:



Examples can be removed and additional lines added as needed.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Email received from client requesting service*	*Collection*	*26(c)*
2.	*Email client back requesting more information*	*Disclosure*	*33.1(7)*
3.	*Service request transferred to service provider contracted by public body*	*Disclosure & Use*	*33.2(c) and 32(a)*

9. Risk Mitigation Table

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Oath of Employment; contractual terms, etc.*	*Low*	*High*
2.	*Request may not actually be from client (i.e. their email address may be compromised)*	*Implementation of identification verification procedures*	*Low*	*High*
3.	*Client's personal information is compromised when transferred to the service provider*	*Transmission is encrypted and over a secure line*	*Low*	*High*
4.	*Inherent risks in sending personal information to a client via email*	*Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail*	*Medium*	*Medium*

10. Collection Notice

If your initiative is collecting personal information directly from individuals you must ensure that all individuals involved are told the following:

1. *The purpose for which the information is being collected*
2. *The legal authority for collecting it, and*
3. *The title, business address and business telephone number of an officer or employee who can answer questions about the collection.*

Please include your proposed wording for a collection notice and where it will be located for individuals to read before collection takes place. You can also attach a screen shot or a copy of your form where the collection notice would be located. For further help with collection notices please see the "Collection Notice Tip Sheet" located on the CIO's website.

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

11. **Please describe the physical security measures related to the initiative (if applicable).**

For example: locked cabinets, securely stored laptops, or key card access to the building.

12. Please describe the technical security measures related to the initiative (if applicable).

For example: use of firewalls, document encryption, or user access profiles assigned on a need-to-know basis.

13. Does your branch/department rely on any security policies?

Please describe any specific policies and procedures and provide contact details for someone who could answer further questions regarding these policies and procedures.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

For example: role-based access.

15. Please describe how you track who has access to the personal information.

For example: audit trails or physical sign-in and sign-out of files.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

For example: users have access to update their own information or, notes will be made on a case file.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

For example: check to see that the information was obtained from a reputable source such as another government agency.

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please describe retention schedules that apply where retention exceeds the one year requirement of FOIPPA. Please contact your public body's privacy office(r) and/or records office(r) if you require assistance.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

For example: your department has a regular exchange of personal information (both collection and disclosure) with the federal government in order to provide services to your clients.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

For example: your public body will be disclosing information to PhD students so that they can conduct research.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Privacy Officer/Privacy Office Representative	Signature	Date

Part 7 – Program Area Signatures

Program/Department Manager	Signature	Date
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Head of Public Body, or designate	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.