qathet
REGIONAL DISTRICT

PRIVACY MANAGEMENT PROGRAM

CONTENTS

OVERVIEW

The purpose of the qathet Regional District's (qRD) Privacy Management Program is to describe how the qRD collects, uses, discloses, and protects personal information. This program outlines how the qRD will ensure personal information is managed in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA). Section 36.2 of FIPPA requires the head of a public body to develop a privacy management program for the public body and to do so in accordance with the directions of the minister responsible for FIPPA.

DEFINITIONS

Contact Information: means information that enables an individual at a place of business to be contacted and includes the name, position or title, business telephone number, business address, business email, or business fax number of the individual.

Data-linking: means the linking, temporarily or permanently, of two (2) or more data sets using one or more common keys.

Employee: in relation to a public body, includes (a)a volunteer, and (b)a service provider.

Personal Information: means recorded information about an identifiable individual other than Contact Information.

Public Body: means a ministry of the government of British Columbia, an agency, board, commission, corporation, office, or other body designated in, or added by regulation to, or a local public body, but does not include the office of a person who is a member or officer of the Legislative Assembly, Court of Appeal, Supreme Court, or Provincial Court.

Privacy Breach: means the theft or loss, or the collection, use, or disclosure, which is not authorized by FIPPA, of personal information in the custody or under the control of a public body.

Privacy Risk: means an inherent risk of unauthorized collection, use, disclosure, or storage of personal information, and something that may inappropriately override or otherwise limit personal privacy.

qathet Regional District: means the local government authority serving five rural electoral areas and one municipality in the qathet region, also referred to as “qRD”.

Record: includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other item on which information is recorded or stored by graphic, electronic, mechanical, or other means, but does not include a computer program or any other mechanism that produces records.

Service Provider: means a person retained under a contract to perform services for a public body.

Third Party: in relation to a request for access to a record or for correction of personal information, means any person, group of persons, or organization other than
(a) the person who made the request, or (b) a public body.

PRIVACY LEAD

In accordance with Section 66 of FIPPA and qathet Regional District Bylaw. No. 272, 1975, the Manager of Administrative Services / Corporate Officer is designated by the Chief Administrative Officer, to be responsible for the following:

- Being a point of contact for privacy-related matters such as privacy questions or concerns;
- Supporting the development, implementation, and maintenance of privacy policies and/or procedures; and
- Supporting the public body's compliance with FIPPA.

Privacy Lead:

Michelle Jones, Manager of Administrative Services
E-mail: administration@qathet.ca
Phone: 604-485-2260

Secondary:

Esme Sturton, Assistant Manager of Administrative Services
E-mail: administration@qathet.ca
Phone: 604-485-2260

Additional Contacts

Chief Administrative Officer:

Al Radke, Chief Administrative Officer
E-mail: administration@qathet.ca
Phone: 604-485-2260

Privacy and Access Helpline:

E-mail: Privacy.Helpline@gov.bc.ca
Phone: 250-356-1851

Office of the Information and Privacy Commissioner for British Columbia:

PO Box 9038 Stn. Prov. Govt.
Victoria B.C. V8W 9A4

E-mail: info@oipc.bc.ca
Phone: (250) 387-5629

PRIVACY IMPACT ASSESSMENTS AND INFORMATION SHARING AGREEMENTS

A process for completing and documenting privacy impact assessments as required and information-sharing agreements as appropriate under FIPPA.

What is a Privacy Impact Assessment (PIA)?

A privacy impact assessment (PIA) is a step-by-step review process to make sure you protect the personal information you collect or use in your project. Doing a PIA can help you protect privacy and build public trust by being clear about what information is being collected, who has access to it, and where and how it's stored. Section 69 (5) of FIPPA requires you to conduct a PIA. You need a PIA to determine whether your project involves personal information and if so, how you'll protect the information you collect or use in your project.

When must you do a PIA?

A head of a public body must conduct a PIA on a new initiative for which no PIA has previously been conducted. A head of a public body must conduct a PIA before implementing a significant change to an existing initiative, including but not limited to, a change to the location in which sensitive personal information is stored, and when it is stored outside of Canada.

Process for Completing a PIA:

- **Step One:** Download the Privacy Impact Assessment Template from New System.
- **Step Two:** Fill out the Privacy Impact Assessment Template with help from the Corporate Officer and Assistant Manager of Administrative Services.
- **Step Three:** Submit to the Corporate Officer and Chief Administrative Officer for review.
- **Step Four**: Get signatures and approval.
- **Step Five:** Start your project.

What is an Information Sharing Agreement?

An Information Sharing Agreement (ISA) is an agreement between a public body and another public body, person or group of persons, prescribed entity, or organization that sets the conditions on the collection, use, or disclosure of personal information by the parties to the agreement. These conditions support compliance with the provisions of FIPPA, other applicable legislation, and relevant policy requirements.

An ISA is an important tool for documenting information sharing conditions, demonstrating compliance with FIPPA and other legislation when required, outlining each party's responsibilities respecting the handling and security of personal information, building a trusted information sharing relationship, and harmonizing expectations for public bodies subject to different policies or legislation. An ISA does not provide the authority to share personal information. Rather, it documents the conditions for information sharing that is otherwise authorized by FIPPA and other applicable law.

Similar to Privacy Impact Assessments, ISAs help to demonstrate compliance with FIPPA or other applicable law and support public bodies in ensuring they are adequately protecting personal information in their custody or under their control. PIAs should be completed for the activities covered by an ISA, rather than each individual ISA.

Process for Completing an ISA:

- **Step One:** Download the Information Sharing Agreement Template from New System.
- **Step Two:** Fill out the Information Sharing Agreement Template with help from the Corporate Officer and Assistant Manager of Administrative Services.
- **Step Three:** Submit to the Corporate Officer and Chief Administrative Officer for review.
- **Step Four**: Get signatures and approval.
- **Step Five:** Start your project.

PRIVACY COMPLAINTS AND PRIVACY BREACHES

Privacy Complaint Procedure

The qRD will follow the procedure outlined in qathet Regional District Policy No. 2.11: *General Complaints Policy*. Privacy complaints should be sent to the Privacy Lead using the form in qathet Regional District Policy No. 2.11: *General Complaints Policy* and will be processed in accordance with its process.

Breach Management Procedure

1. Notify the Privacy Lead and all relevant personnel. This should include the head of the relevant department, the IT security team, and the designated incident response team.

2. The Privacy Lead and relevant personnel will assess the nature and scope of the breach. This should include determining what information was accessed, who may have been affected, and how the breach occurred.

3. Contain the breach. Where a breach is related to a cyber incident or IT system, qathet Regional District's internal Cyber Security Incident Response Plan must be followed.

4. Begin an investigation to determine the cause of the breach and identify any areas where security measures may have been inadequate.

5. Notify individuals and organizations that may have been affected by the breach in accordance with any legal or regulatory requirements.

6. Provide appropriate assistance to affected individuals, such as offering credit monitoring or identity theft protection services.

7. Review and update security procedures and protocols as needed to prevent similar incidents in the future.

8. Document the entire incident and the steps taken to address it.

9. Report the incident to the relevant regulatory body if required.

PRIVACY AWARENESS AND EDUCATION

Privacy Awareness and Education Procedures

Employees are an important part of breach prevention. The qRD regularly monitors and identifies where in the organization privacy gaps exist. Privacy training and awareness helps employees identify personal information and understand their privacy obligations. Privacy education is incorporated into the onboarding process for new employees. The qRD has partnered with MIABC and runs online training for employees on privacy-related topics such as data protection and cybersecurity.

What is considered personal information?

Personal information includes recorded information that can be used to identify an individual through association or inference. Some examples are:

- name, age, sex, weight, height;
- home address and phone number;
- race, ethnic origin, sexual orientation;
- medical information; and/or
- human resources information.

The following privacy topics for education activities are relevant for most public bodies:

- an understanding of what constitutes personal information;
- appropriate collection, use, and disclosure of personal information;
- reasonable security measures and access controls to protect personal information; and
- identification and reporting of privacy breaches and privacy complaints.

Training on the following topics may also be included:

- PIAs; and
- privacy and security requirements for storage of sensitive personal information outside of Canada.

Employees with access to employee personal information are subject to additional training.

The Privacy Lead distributes educational materials explaining the organization's privacy obligations, policies, and procedures, including:

- Guide to Good Privacy Practices
- FIPPA Foundations: Privacy and Access Fundamentals

THIRD PARTY SERVICE PROVIDER PRIVACY OBLIGATIONS

Third Party Service Provider Privacy Obligations Procedure

Under FIPPA, any service providers have the same privacy obligations as the qRD for the service that they are providing to the qRD under contract. Each department will work with the Corporate Officer to identify which contracts involve the handling of personal data and review the current terms and conditions of these contracts to ensure they are in compliance with relevant privacy laws and regulations.

Contracts and Non-Disclosure Agreements outline the specific privacy obligations that the service provider must adhere to, including data handling, storage, and security requirements. These agreements must include language that requires the service provider to comply with all relevant privacy laws and regulations. Before the contract is executed, service providers are educated about their responsibilities and legal requirements. Each department regularly reviews their service providers' compliance with the privacy requirements outlined in their contract and takes appropriate action if any non-compliance is identified.

PRIVACY PRACTICES AND POLICIES

The qRD is dedicated to ensuring that all its documented privacy processes and practices are available to all qRD employees and, where possible, to the public. The qRD has taken a proactive approach to privacy management which includes privacy practices and procedures in many of our existing policies.

The following privacy policies and procedures are available to the public on our website at qathet.ca or upon request:

- **Bylaw 272:** Freedom of Information and Protection of Privacy
- **Policy 1.10:** Corporate Electronic Device Purchase Policy
- **Policy 2.5:** Information for Educational Purposes
- **Policy 2.6:** Dissemination of Digital Mapping Information
- **Policy 2.9:** Public Communication and Engagement
- **Policy 2.11:** General Complaints Policy
- **Policy 2.12:** Bylaw Complaints and Enforcement
- **Policy 2.13:** Social Media
- **Policy 3.11:** Financial Assistance
- **Policy 4.15:** Vehicle Use Policy
- **Policy 4.16:** Workplace Discrimination and Bullying and Harassment

REGULAR MONITORING AND UPDATING

The qRD is committed to gathering feedback from employees and third-party service providers to address any gaps and implement suggestions in future updates to this procedure guide. The Administrative Services department will be responsible for regularly reviewing and updating this procedure at least annually to ensure that it is in compliance with relevant privacy laws, business practices, and regulations.