qathet
REGIONAL DISTRICT

PRIVACY MANAGEMENT PROGRAM

CONTENTS

OVERVIEW 2

PRIVACY LEAD 3

PRIVACY IMPACT ASSESSMENTS AND INFORMATION SHARING AGREEMENTS 4

PRIVACY COMPLAINTS AND PRIVACY BREACHES 6

PRIVACY AWARENESS AND EDUCATION 7

THIRD PARTY SERVICE PROVIDER PRIVACY OBLIGATIONS 7

PRIVACY PRACTICES AND POLICIES 7

REGULAR MONITORING AND UPDATING 8

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.

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

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.
- **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.
- **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.

Employees are required to participate in Cyber Security Training and FIPPA training as prescribed by the Manager of Technical Services and Manager of Administrative Services.

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

All service providers handling personal information related to the provision of services for the qRD must be informed of their privacy obligations. Training and education is provided, and service providers are required to acknowledge reviewing and understanding all related qRD policies and procedures. All contracts and agreements with service providers will include a privacy protection schedule outlining the obligations and requirements of the service providers to protect privacy and personal information.

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.