

Privacy Management Program Policy 220, 2025

The following was approved by the Chief Administrative Officer (CAO) as an Administrative Policy on **June 17, 2025**.

PURPOSE

[Section 36.2](#) of the *Freedom of Information and Protection of Privacy Act (FOIPPA)* requires the head of a public body to develop a Privacy Management Program (PMP). The Ministry of Citizen's Services [PMP Directions](#) set out the mandatory components and framework of a PMP.

PROGRAM

1. PRIVACY MANAGEMENT PROGRAM (PMP)

- 1.1 The District of Lake Country (the "District") shall collect, use, disclose, protect and manage [personal information](#) (recorded information about an identifiable individual other than business contract information) in accordance with *FOIPPA* as follows:
- (a) An employee, officer or director of a public body or employee of a service provider must not collect, use or disclose personal information except as authorized by *FOIPPA* (s.[25.1](#)).
 - (b) A public body is only permitted to collect personal information in accordance with *FOIPPA* (ss.[26](#), [27](#)).
 - (c) A public body is required to protect personal information in its custody and control by making reasonable security arrangements against unauthorized collection, use, disclosure or disposal (s.[30](#)).
 - (d) A public body may only disclose personal information in accordance with Section [33](#).

2. DESIGNATION

- 2.1 The Corporate Officer, including their deputy, is designated as the head of a public body and responsible for:
- (a) being the point of contact for privacy-related matters such as privacy questions or concerns
 - (b) supporting the development, implementation, and maintenance of privacy policies or procedures, and
 - (c) supporting the public body's compliance with *FOIPPA*

3. PRIVACY IMPACT ASSESSMENT (PIA)

- 3.1 Staff will complete and submit a [PIA](#) to the Corporate Officer where a new project or initiative involves:
- (a) collection of personal information
 - (b) a [data-linking program](#) (linking District data with another public body or agencies data without consent of the individuals whose personal information is in the data), or
 - (c) or [common or integrated program or activity](#) (*provides services through a public body or agency collaboratively, or on behalf of, or is deemed such by regulation*)

- 3.2 The Corporate Officer will review the [PIA](#) and
- (a) approve the project or provide recommendations for proceeding.
 - (b) forward the PIA to the OIPC if the project is a data-linking program, or common or integrated program or activity (*FOIPPA* section [69](#)).
 - (i) Upon receiving advice or recommendations from OIPC, the Corporate Officer will provide directions on how to proceed with the project.

4. INFORMATION SHARING AGREEMENT PROCESS

- 4.1 Where the District plans to share or receive personal information on a one-time transfer or on a recurring basis, the Corporate Officer will enter into an Information Sharing Agreement (ISA) ([Master Template ISA](#)) in accordance with the [Provincial Guidance Document – Information Sharing Agreements](#).
- 4.2 Prior to entering into an ISA, the Corporate Officer will determine if the District has legal authority to disclose or receive the information and security arrangements will be made against unauthorized access.

5. PRIVACY COMPLAINT

- 5.1 Privacy complaints must be submitted to the Corporate Officer in writing.
- 5.2 Upon receipt of a privacy complaint, the Corporate Officer will:
- (a) investigate the complaint;
 - (b) provide written acknowledgment that the complaint has been received to the complainant no later than 15 days from the date of receipt;
 - (c) provide a written response to the complainant including information determined necessary by the Corporate Officer, no later than 30 days from the date of receipt;
 - (d) where a privacy breach is identified, take necessary steps in accordance with Section 6 of this Policy;
 - (e) identify areas for improvement, education and training, where appropriate.
- 5.3 If a complainant is not satisfied with the response from the Corporate Officer, they may request a review, in writing to the CAO. The CAO may recommend further action, including, but not limited to, a written response to the complainant, an additional investigation and report by the Corporate Officer or other steps as determined appropriate by the CAO.

6. PRIVACY BREACH

- 6.1 Council, staff, volunteers and service providers have a duty to report suspected or actual privacy breaches (inadvertent or intentional) to their supervisor or manager, or the Corporate Officer.
- 6.2 Where the Corporate Officer is advised of a privacy breach, they will take immediate steps to contain the breach including requesting assistance from the Information Technology Department and the [OIPC Privacy breaches tools and resources for public bodies](#).

- 6.3 Where a privacy breach has been determined to have occurred, the Corporate Officer will complete the [OIPC Privacy Breach Checklist for Public Bodies](#) and undertake the following actions:
- (a) Contain the breach (immediate)
 - (b) Report the breach (staff to supervisor, Supervisor to Corporate, Corporate to Mayor etc.)
 - (c) Preserve evidence
 - (d) Contact police if appropriate
 - (e) Conduct analysis of risks and cause of breach
 - (f) Determine if the breach should be reported to the Privacy Commissioner
 - (g) Determine if notification of affected individuals is necessary
 - (h) Review investigative finding and develop prevention strategies
 - (i) Implement prevention
 - (j) Monitor prevention strategies
- 6.4 Depending on the severity of the breach, the OIPC may be notified by completing an online [Privacy Breach Report](#). Where the internal report indicates affected individuals should be notified, the Corporate Officer will advise individuals of the breach by phone, letter or in person, unless notification could cause further harm, is cost prohibitive or the contact information is unavailable.

7. PRIVACY AWARENESS AND EDUCATION

- 7.1 Privacy awareness and educational activities for employees will take place as follows:

ACTIVITY	TIMELINE
Posting information on the intranet	Every 6 months
In person training sessions	Once a year
Requirement to complete online privacy assessment course	Once a year

8. PRIVACY POLICIES, PROCESSES AND PRACTICES

- 8.1 Privacy policies and procedures available to staff include:
- (a) [Information Bulletin - Personal Information](#)
 - (b) [Information Bulletin - FOI](#)
 - (c) [Code of Ethics Policy 2013.130](#)
 - (d) [Website privacy policy](#)

9. DISTRICT FORMS

- 9.1 The District will include the following privacy statement on forms collecting [personal information](#):

"The [personal information](#) on this form is collected under the authority of British Columbia's Freedom of Information and Protection of Privacy Act. Any questions regarding this collection of information should be directed to the Corporate Officer, District of Lake Country, 10150 Bottom Wood Lake Rd., V4V 2M1, Phone 778-766-5650 or admin@lakecountry.bc.ca"

10. SERVICE PROVIDERS

- 10.1 To ensure service providers are informed of their privacy obligations, the District will ensure all contracts and agreements include service providers acknowledgement of their privacy responsibilities and obligations under the [Personal Information and Protection Act \(PIPA\)](#).

11. CORRECTION OF PERSONAL INFORMATION ([FOIPPA s. 29](#))

- 11.1 Upon receipt of a request to correct an individual's personal information on records within the custody or control of the District, staff will:
- (a) ensure identity of requestor is verified
 - (b) correct the information as requested or annotate that no correction was made
 - (c) notify other public bodies or third parties who have received the personal information within one year prior to the date of the request, of the request to correct the personal information
 - (d) with 30 days from the date of the request, the Corporate Officer will provide a response to the individual that the information has been corrected, third parties have been notified and/or reasons why the request could not be accommodated

12. VERIFICATION OF IDENTITY

- 12.1 Staff will request verification of identity as follows:
- (a) Where an individual requests their own personal information staff will ask for additional identification.
 - (b) Where a third-party requests another individual's personal information they must provide written consent or proof of verification to act on behalf of the individual.
 - (c) Where an individual requests their own personal information via email, staff will call the individual to confirm the request.
- 12.2 Identity can be verified by:
- (a) confirming 3 pieces of information contained within a District file that are not public information
 - (b) providing photo identification, or
 - (c) providing identification with a signature that matches information on a District file

13. MONITORING AND UPDATING

- 13.1 This policy will be reviewed every two years or when an amendment occurs within legislation to ensure that the District of Lake Country is compliant with *FOIPPA*.

14. APPROVALS, AMENDMENTS AND ANNUAL REVIEWS

Date	Approver	Type
February 2, 2026	Reyna Seabrook	Amendment

"original signed by Paul Gipps"

Chief Administrative Officer

February 2, 2026

Date