A-41 Policy – Privacy Management Program and Privacy Breach Policy

Preamble: This policy provides a framework for how the Central Coast Regional District (CCRD) operates to ensure that Personal Information is managed in accordance with the *Freedom of Information and Protection of Privacy Act*.

Policy: The purpose of the CCRD's Privacy Policy is to describe how the CCRD collects, uses, discloses, and protects personal information. This policy applies to Personal Information that the CCRD collects, uses, or discloses in any form (including verbal, electronic, or written Personal Information). This policy is the foundation for the CCRD's Privacy Management Program.

Definitions:

Act means the *Freedom of Information and Protection of Privacy Act* (British Columbia) as may be amended or replaced from time to time.

Commissioner means the Information and Privacy Commissioner for the Province of British Columbia.

Employee means an employee of the CCRD, including a volunteer or service provider.

Information Sharing Agreement or ISA means an agreement between the CCRD 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.

Personal Information means recorded information about an identifiable individual (but does not include information to enable an individual at a place of business to be contacted, such as the name, position name or title, business telephone number, business address, business email, or business fax number of the individual).

Privacy Impact Assessment or PIA means an assessment that is conducted by the CCRD to determine if a current or proposed enactment, system, project, program, or activity meets or will meet the requirements of Part 3 of the *Act.*

Privacy Officer means the Corporate Administrator or delegate who is responsible for being the primary contact for privacy-related matters and supporting the CCRD's compliance with the *Act.*

Service Provider means a person or organization retained under a contract to perform services for the CCRD.

1. Collection of Personal Information

(1) The CCRD may collect Personal Information:

(a) where the collection is authorized under a statute, such as the *Community Charter* and the *Local Government Act* or is authorized under CCRD bylaws;

(b) for the purposes of CCRD activities, services, and programs;

(c) for the purposes of planning or evaluating CCRD activities, services, and programs;

(d) for law enforcement purposes, including enforcing the CCRD's bylaws; and

(e) at presentations, ceremonies, performances, sports meets, or similar events, that are open to the public and where individuals voluntarily appear, such as public meetings and public hearings.

(2) The CCRD collects Personal Information directly from individuals but may also collect information from another source if an individual has consented to the CCRD in doing so. The CCRD may also collect Personal Information from another source as permitted under the *Act*, including in these cases:

(a) where another law allows the CCRD to do so;

(b) for law enforcement, for a court proceeding, to collect a debt or fine, or to make a payment;

(c) where Personal Information is necessary for the CCRD to deliver, or evaluate, a common or integrated program or activity;

(d) where Personal Information is necessary to establish, manage, or terminate an employment relationship between the CCRD and an individual;

(e) if Personal Information may be disclosed to the CCRD under Part 3 of the *Act*; or

(f) where the CCRD collects Personal Information for the purpose of determining a person's suitability for an honour or award.

(3) The CCRD will endeavor to limit the amount of Personal Information recorded to that which is necessary to fulfill the purpose for which the information is being collected.

2. Use and Disclosure of Personal Information

(1) The CCRD will use and disclose Personal Information only for the purpose the CCRD collected it for or for a purpose that is consistent with why the CCRD collected it in the first place.

(2) The CCRD may also use or disclose Personal Information for another purpose if an individual has identified the information and consented to the CCRD's other use.

(3) The CCRD may use Personal Information for a purpose for which the information can be disclosed to the CCRD under Part 3 of the *Act.*

(4) The CCRD may also disclose a person's Personal Information:

(a) if the person has identified the information and consented in writing to its disclosure;

(b) to the CCRD's Employees if the information is necessary for their duties, for delivery of a common or integrated program or activity, or for planning or evaluating a CCRD program or activity;

(c) if the Personal Information is made publicly available in British Columbia by a law that authorizes or requires it to be made public;

(d) to a public body or law enforcement agency to assist in a specific investigation or law enforcement proceeding;

(e) to a person's union representative who is making an inquiry, if the person has given the representative written authority to make the inquiry, or it is otherwise authorized;

(f) to the CCRD's legal counsel for the purpose of legal advice or for use in legal proceedings involving the CCRD;

(g) to a person's Member of the Legislative Assembly (MLA) if the person has asked the MLA to help resolve a problem; or

(h) as otherwise permitted or required under Part 3 of the *Act*.

(5) All information provided at open board meetings or its committees/commissions is considered to be public. If a person provides or discloses their Personal Information to the CCRD for that purpose, the person consents to that information being available to the public, including through posting on the CCRD's website or webcasting. This information is considered to be a part of the public record and cannot be removed or changed. However, if a person satisfies the CCRD in advance that the person has legitimate personal safety concerns for themselves or an immediate family member, the CCRD may allow the person to submit their Personal Information to the Board of

Directors or a Committee/Commission in confidence. The CCRD will not make the Personal Information publicly available in that instance.

3. Accuracy of Personal Information

(1) The CCRD will make every reasonable effort to ensure that the Personal Information the CCRD uses to make a decision directly affecting a person is accurate and complete.

4. Access to Personal Information

(1) A person can ask the CCRD to give them a copy of their Personal Information that is in the CCRD's custody or control by contacting the Corporate Administration department.

(2) If an Employee of the CCRD would like a copy of their own employee's Personal Information, the Employee will need to contact the Corporate Administration department.

(3) If the CCRD believes a person's request may involve someone else's Personal Information, or information protected under the *Act*, the CCRD may require the person to make a formal request under the *Act* for access to those records. In some cases, the *Act* may require the CCRD to refuse access to a person's own Personal Information. The CCRD will give the requestor written reasons for every decision on a formal request.

(4) Before disclosing a person's Personal Information, the CCRD will require the person to verify their identity, so the CCRD can be assured that the requestor is the individual whose information is being requested. This helps ensure that the CCRD does not disclose a person's Personal Information to someone to whom it should not be given.

5. Correction of Personal Information

(1) If a person believes there is an error or omission in or from their Personal Information, the person can contact the CCRD in writing and ask the CCRD to correct it. If the CCRD decides to correct that information, the CCRD will do so as soon as reasonably possible. If the CCRD decides not to correct the information, the CCRD will note the requested change in the information as well as why the CCRD did not correct the information as requested.

6. Retention and Disposal of Personal Information

(1) If the CCRD uses Personal Information to make a decision that directly affects a person, the CCRD will keep the information for at least one year after the CCRD makes the decision.

(2) The CCRD shall keep Personal Information in accordance with the CCRD's relevant record retention schedules.

(3) The CCRD will use reasonable efforts to ensure that Personal Information is destroyed securely under the CCRD's records retention schedules.

7. Responsible Use of Information and Information Technology

(1) The CCRD will use what the CCRD believes are reasonable security arrangements to protect a person's Personal Information against such risks as unauthorized access, collection, use, and disclosure. These arrangements may include information technology measures, as well as policies and practices, to protect a person's Personal Information.

(2) If the CCRD discloses a person's Personal Information to one of the CCRD's service providers, the CCRD will make reasonable efforts to impose contractual protections on the service provider. Those protections vary according to the nature and sensitivity of the Personal Information involved. The CCRD requires the CCRD's service providers not to use or disclose Personal Information other than for the purpose of performing services for the CCRD.

(3) All CCRD Employees are required to respect the confidentiality of Personal Information they receive or compile and are required to use and disclose it only in accordance with this policy and the *Act*.

8. Responding to Privacy-Related Complaints

(1) The procedure for registering a privacy complaint with the CCRD is outlined in Appendix A attached to this policy.

9. Education and Awareness

(1) All CCRD Employees receive training on the *Act* and privacy generally as appropriate to their work function. Additional training is given in the following circumstances:

(a) Employees handling what the CCRD considers high-risk or sensitive Personal Information electronically receive training related to information systems and their security;

(b) Employees managing programs or activities receive training related to Privacy Impact Assessments; and

(c) Employees managing common or integrated programs or activities receive training related to information-sharing agreements.

10. Privacy Impact Assessments (PIA)

(1) A PIA will be conducted for any new system, project, program, or activity involving Personal Information and for any new collection, use, or disclosure of Personal Information. A template PIA can be found in Appendix C.

(2) A PIA will be conducted for common or integrated programs or activities and data-linking initiatives, as well as when significant modifications are made to existing systems, projects, programs, or activities.

11. Information Sharing Agreements (ISA)

(1) If the CCRD is sharing personal information with an organization, public body, or agency external to the CCRD, the Employee responsible for that program or activity should, where applicable, complete the ISA template in Appendix D of this policy, and any further directions provided by the Privacy Officer.

(2) An ISA is considered to be completed once it has been fully signed by all of the required parties.

(3) Any Employee completing an ISA will ensure that the Privacy Officer is consulted throughout the process and promptly provided with a copy of the completed ISA.

12. Privacy Breach Management and Protocols

(1) The procedures for responding to a privacy breach are outlined in Appendix A of this policy.

13. Service Provider Management

(1) Employees who prepare or manage contracts with service providers shall include the Privacy Protection Schedule in all contracts that involve the service provider having access to, or collecting, using, or disclosing, Personal Information in the custody or under the control of the CCRD. The Privacy Protection Schedule is included as Appendix B of this policy.

14. External Communications

(1) Under this policy, the CCRD will contact an individual in the following circumstances:

(a) to give notice of the collection of their Personal Information;

(b) when individuals request access to their Personal Information or access to records where someone else's Personal Information is involved;

(c) when responding to requests for correction of Personal Information;

(d) when Personal Information is disclosed without consent for compelling health or safety reasons; and

(e) when the CCRD intends to give access to Personal Information in response to a freedom of information request.

15. Authority to Act

(1) The Corporate Officer is delegated responsibility and authority for ensuring compliance with this policy and the *Act.*

Adopted: March 28, 2024 Resolution: 24-03-16

APPENDIX A

Procedures for Managing Privacy Breaches

1. Privacy Complaints and Breaches

1.1 Any complaint about any privacy-related matter under this policy or under the *Act* must be made to the CCRD in writing.

1.2. The CCRD will consider a person's complaint, including about a breach of the person's privacy, and will disclose the outcome to the person in writing. The CCRD expects a complainant to co-operate reasonably and in a timely way with the CCRD's work, including by promptly providing the CCRD with information that the CCRD might reasonably need to do the CCRD's work. A complainant's failure to do so may result in the CCRD's deciding not to proceed any further with the complaint.

1.3. A person may make a written formal complaint to the Office of the Information and Privacy Commissioner for British Columbia, although the CCRD encourages individuals to use the CCRD's complaint procedure first. Wherever possible, the CCRD will endeavor to work things out directly with people to their satisfaction.

2. Requirement to Notify

2.1 Upon notice of a privacy breach, the Privacy Officer shall be contacted, in writing, without unreasonable delay.

2.2 The Privacy Officer shall, without unreasonable delay;

2.2.1 notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including:

2.2.1.1. identity theft or significant bodily harm,

2.2.1.2. humiliation,

2.2.1.3. damage to reputation or relationships,

2.2.1.4. loss of employment, business or professional opportunities,

2.2.1.5. financial loss,

2.2.1.6. negative impact on a credit record, or

2.2.1.7. damage to, or loss of, property.

2.2.2 notify the Commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph 2.2.1 above.

3. Notification Procedure

3.1 Direct Notification for Affected Individuals

3.1.1 Notifications must include the following information:

3.1.1.1. the name of the public body;

3.1.1.2. the date on which the privacy breach came to the attention of the public body;

3.1.1.3. a description of the privacy breach including, if known,

3.1.1.4. the date on which or the period during which the privacy breach occurred, and

3.1.1.5. a description of the nature of the Personal Information involved in the privacy breach;

3.1.1.6. confirmation that the Commissioner has been or will be notified of the privacy breach (per section 2.2.2 of this appendix);

3.1.1.7. contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;

3.1.1.8. a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;

3.1.1.9. a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

3.2. Indirect Notifications for Affected Individuals

3.2.1 A notification may be given to an affected individual in an indirect manner if:

3.2.1.1. the public body does not have accurate contact information for the affected individual,

3.2.1.2. the head of the public body reasonably believes that providing the notice directly to the affected individual would unreasonably interfere with the operations of the public body, or

3.2.1.3. the head of the public body reasonably believes that the information in the notification will come to the attention of the affected individual more quickly if it is given in an indirect manner.

3.2.2 If a notification must be given in an indirect manner, the notification must:

3.2.2.1. be given by public communication that can reasonably be expected to reach the affected individual, and

3.2.2.2. contain the following information:

a. the name of the public body;

b. the date on which the privacy breach came to the attention of the public body;

c. a description of the privacy breach including, if known,

(i) the date on which or the period during which the privacy breach occurred, and

(ii) a description of the nature of the Personal Information involved in the privacy breach;

d. confirmation that the Commissioner has been or will be notified of the privacy breach;

e. contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;

f. a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;

g. a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

3.3. Notifications to the Commissioner

3.3.1 A notification to the Commissioner under section 36.3 (2)(b) of the *Act* must be given to the Commissioner in writing and must include the following information:

3.3.1.1. the name of the public body;

3.3.1.2. the date on which the privacy breach came to the attention of the public body;

3.3.1.3. a description of the privacy breach including, if known, a. the date on which or the period during which the privacy breach occurred, b. a description of the nature of the Personal Information involved in the privacy breach, and c. an estimate of the number of affected individuals;

3.3.1.4. contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;

3.3.1.5. a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.

3.4. Not Required to Notify

3.4.1 Per section 36.3(3) of the *Act*, "the head of a public body is not required to notify an affected individual under subsection (2) if notification could reasonably be expected to

3.4.1.1. result in immediate and grave harm to the individual's safety or physical or mental health, or

3.4.1.2. threaten another individual's safety or physical or mental health."

3.5. Disregarding Requests

3.5.1 If the Privacy Officer asks, the Commissioner may authorize the public body to disregard a request if:

3.5.1.1. a request is frivolous or vexatious,

3.5.1.2. a request is for a record that has been disclosed to the applicant or that is accessible by the applicant from another source, or

3.5.1.3. responding to the request would unreasonably interfere with the operations of the public body because the request:

a. is excessively broad, or

b. is repetitious or systematic.

APPENDIX B

Privacy Protection Schedule

Definitions

1. In this Schedule,

   (a) "***Act***" means the *Freedom of Information and Protection of Privacy Act* including any regulation made under it;

   (b) "**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 email or business fax number of the individual;

   (c) "**Personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Central Coast Regional District and the Contractor dealing with the same subject matter as the Agreement;

   (d) "**Privacy course**" means the CCRD's online privacy and information sharing training course, or another course approved by the Province; and

   (e) "**Public body**" means "public body" as defined in the *Act*;

   (f) "**Third party request for disclosure**" means a subpoena, warrant, order, demand or request from an authority inside or outside of Canada for the unauthorized disclosure of personal information to which the *Act* applies;

   (g) "**Service provider**" means a person retained under a contract to perform services for a public body; and

   (h) "**Unauthorized disclosure of personal information**" means disclosure of production of or the provision of access to personal information to which the *Act* applies, if that disclosure, production or access is not authorized by the *Act*.

Purpose

2. The purpose of this Appendix is to:

   (a) enable the Central Coast Regional District (CCRD) to comply with the CCRD's statutory obligations under the *Act* with respect to personal information; and

(b) ensure that, as a service provider, the Contractor is aware of and complies with the Contractor's statutory obligations under the *Act* with respect to personal information.

Acknowledgements

3. The Contractor acknowledges and agrees that:

(a) it is a service provider and, as such, the requirements and restrictions established by Part 3 of the *Act* apply to the Contractor in respect of personal information;

(b) unless the Agreement otherwise specifies, all personal information in the custody of the Contractor is and remains under the control of the CCRD; and

(c) unless the Agreement otherwise specifies or the CCRD otherwise directs in writing, the Contractor may only collect, use, disclose, or store personal information that relates directly to and is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Collection of Personal Information

4. The Contractor must collect personal information directly from the individual that the information is about unless:

(a) the CCRD provides personal information to the Contractor;

(b) the Agreement otherwise specifies; or

(c) the CCRD otherwise directs in writing.

5. Where the Contractor collects personal information directly from the individual the information is about, the Contractor must tell that individual:

(a) the purpose for collecting it;

(b) the legal authority for collecting it; and

(c) the contact information of the individual designated by the CCRD to answer questions about the Contractor's collection of personal information.

Privacy Training

6. The Contractor must ensure that each individual who will provide services under the Agreement that involve the access, collection, or creation of personal information will complete, at the Contractor's expense, the privacy course prior to that individual providing those services.

7. The requirement in section 7 will only apply to individuals who have not previously completed the privacy course.

Accuracy of Personal Information

8. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the CCRD to make a decision that directly affects the individual the information is about.

Requests for Access to Information

9. If the Contractor receives a request for access to information from a person other than the CCRD, the Contractor must promptly advise the person to make the request to the CCRD unless the Agreement expressly requires the Contractor to provide such access. If the CCRD has advised the Contractor of the name or title and contact information of an official of the CCRD to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of Personal Information

10. Within 5 Business Days of receiving a written direction from the CCRD to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

11. When issuing a written direction under section 11, the CCRD must advise the Contractor of the date the correction request was received by the CCRD in order that the Contractor may comply with section 13.

12. Within 5 Business Days of correcting or annotating any personal information under section 11, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was received by the CCRD, the Contractor disclosed the information being corrected or annotated.

13. If the Contractor receives a request for correction of personal information from a person other than the CCRD, the Contractor must promptly advise the person to make the request to the CCRD and, if the CCRD has advised the Contractor of the name or title and contact information of an official of the CCRD to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of Personal Information

14. Without limiting any other provision of the Agreement, the Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including without limitation by ensuring that the integrity of the personal information is preserved. Without limiting the general nature of the foregoing sentence, the Contractor will ensure that all personal information is securely segregated from any information under the control of the Contractor or third parties to prevent unintended mixing of personal information with other information or access to personal information by unauthorized persons and to enable personal information to be identified and separated from the information of the Contractor or third parties.

Storage of and Access to Personal Information

15. The Contractor must comply with the requirements under the *Act* concerning storage of personal information outside of Canada, including, if required by the CCRD, by supporting the CCRD with completion of such assessments as may be required by law.

16. The Contractor must not change the location where personal information is stored without receiving prior authorization of the CCRD in writing.

17. Without limiting any other provision of the Agreement, the Contractor will implement and maintain an access log documenting all access to personal information, including a list of all persons that access any personal information. The Contractor will provide a copy of the access log to the CRRD upon request.

Retention of Personal Information

18. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the CCRD in writing to dispose of it or deliver it as specified in the direction.

Use of Personal Information

19. Unless the CCRD otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement. For clarity, unless the Agreement otherwise specifies or the CCRD otherwise directs in writing, the Contractor must not anonymize, aggregate, or otherwise alter or modify personal information, including by converting personal information into non-personal information, or analyze personal information (whether by manual or automated means) for any purpose, including for the purpose of developing insights, conclusions or other information from personal information.

Metadata

20. Where the Contractor has or generates metadata as a result of services provided to the CCRD, where that metadata is personal information, the Contractor will:

(a) not use it or disclose it to any other party except where the Agreement otherwise specifies; and

(b) remove or destroy individual identifiers, if practicable.

Disclosure of Personal Information

21. Unless the CCRD otherwise directs in writing, the Contractor may only disclose personal information to any person other than the CCRD if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

22. If in relation to personal information, the Contractor:

(a) receives a third-party request for disclosure;

(b) receives a request to disclose, produce, or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a third-party request for disclosure; or

(c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a third-party request for disclosure,

Subject to section 24, the Contractor must immediately notify the CCRD.

23. If the Contractor receives a third-party request described in section 23(a) or (b) but is unable to notify the CCRD as required by section 23, the Contractor must instead:

(a) use its best efforts to direct the party making the third-party request to the CCRD;

(b) provide the CCRD with reasonable assistance to contest the third-party request; and

(c) take reasonable steps to challenge the third party-request, including by presenting evidence with respect to:

(i) the control of personal information by the CCRD as a public body under the *Act*;

(ii) the application of the *Act* to the Contractor as a service provider to the CCRD;

(iii) the conflict between the *Act* and the third-party request; and

(iv) the potential for the Contractor to be liable for an offence under the *Act* as a result of complying with the third-party request.

Notice of Unauthorized Disclosure

24. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the *Act*, if the Contractor knows that there has been an unauthorized disclosure of personal information, the Contractor must immediately notify the CCRD.

Compliance with the *Act* and Directions

25. The Contractor must in relation to personal information comply with:

1. the requirements of the *Act* applicable to the Contractor as a service provider, including any regulation made under the *Act* and the terms of this Schedule; and
2. any direction given by the CCRD under this Schedule.

26. The Contractor acknowledges that it is familiar with the requirements of the *Act* governing personal information that are applicable to it as a service provider.

27. The Contractor will provide the CCRD with such information as may be reasonably requested by the CCRD to assist the CCRD in confirming the Contractor's compliance with this Schedule.

Notice of Non-Compliance

28. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply in any respect, with any provision in this Schedule, the Contractor must promptly notify the CCRD of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

29. In addition to any other rights of termination which the CCRD may have under the Agreement or otherwise at law, the CCRD may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

30. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

31. Any reference to "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with the requirements of the *Act* applicable to them.

32. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

33. If a provision of the Agreement (including any direction given by the CCRD under this Schedule) conflicts with a requirement of the *Act*, including any regulation made under the *Act*, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

34. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of the Agreement or the law of any jurisdiction outside Canada.

35. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the *Act*.

APPENDIX C

Privacy Impact Assessment Template

Table of Contents

Use this privacy impact assessment (PIA) template if you work for or are a service provider to the Central Coast Regional District (CCRD) and are starting a new initiative or significantly changing an existing initiative.

Before you start

- An initiative is an enactment, system, project, program or activity.
- If you have any questions, contact the CCRD Privacy/Corporate Officer.

PART 1: GENERAL INFORMATION

Initiative title:	
Organization:	Central Coast Regional District
Department:	
Your name and title:	

Your work phone:	
Your email:	
Initiative Lead name and title:	
Initiative Lead phone:	
Initiative Lead email:	

The CCRD Privacy Officer will complete the questions in the table below.

Is this initiative a data-linking program under *FOIPPA*? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
Is this initiative a common or integrated program or activity? Under section *FOIPPA 69 (5.4)*, you must submit this PIA to the Office of the Information and Privacy Commissioner.
Related PIAs, if any:

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs. Reports are generated with this information.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

PART 1: GENERAL INFORMATION

What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Type "YES" or "NO" to indicate your response.

- If YES, go to Part 2.
- If NO, answer Question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template**.**

How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

Collection, use and disclosure - To be filled out by Privacy/Corporate Officer

Use Column 2 to identify whether the action in Column 1 is a collection, use or disclosure of personal information. Use Columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	***FOIPPA* authority**	**Other legal authority**
Step 1:			
Step 2:			
Step 3:			
Step 4:			
Step 1:			

Optional: Insert a drawing or flow diagram here or in an Appendix if you think it will help to explain how each different part is connected.

Collection Notice

If you are collecting personal information directly from an individual the information is about, *FOIPPA* requires that you provide a collection notice (except in limited circumstances). Review the sample collection notice and write your collection notice below. You can also attach the notice as an appendix.

For example: "The personal information you provide on this site is being collected in accordance with the *Freedom of Information and Protection of Privacy Act* and will be used only for the purpose of processing CCRD business. If you have any questions about the collection of your personal information, please contact the Central Coast Regional District at info@ccrd.ca or call 250-799-5291 and request the Privacy Officer/Corporate Officer."

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

Is any personal information stored outside of Canada?

Type "YES" or "NO" to indicate your response.

Where are you storing the personal information involved in your initiative?

Does your initiative involve sensitive personal information?

Type "YES" or "NO" to indicate your response.

- If YES, go to Question 10.
- If NO, go to Part 5.

Is the sensitive personal information being disclosed outside of Canada under *FOIPPA section 33(2)(f)*?

Type "YES" or "NO" to indicate your response.

- If YES, go to Part 5.
- If NO, go to Part 4.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. More help is available in the Guidance on Disclosures Outside of Canada.

Is the sensitive personal information stored by a service provider?

Type "YES" or "NO" to indicate your response.

- If YES, fill in the table below (add more rows if necessary) and go to Question 13
- If no, go to Question 12.

Name of service provider	**Name of cloud infrastructure and/or platform provider(s) (if applicable)**	**Where is the sensitive personal information stored (including backups)?**

Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

Does the contract you rely on include privacy-related terms?

Type "YES" or "NO" to indicate your response.

- If YES, describe the contractual measures related to your initiative.

What controls are in place to prevent unauthorized access to sensitive personal information?

Provide details about how you will track access to sensitive personal information.

15. Describe the privacy risks for disclosure outside of Canada.

Use the table below to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed. This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response** **(this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk?** **If yes, please describe.**

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the Privacy Officer on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The CCRD may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

This part captures information about the privacy aspects of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical (e.g., your office building or work environment) and technical (e.g., online cloud service) environments.

16. Does your initiative involve digital tools, databases, or information systems?

Type "YES" or "NO" to indicate your response.

- If YES, determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of *FOIPPA section 30*.

16.1 **Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of *FOIPPA section 30*?**

Type "YES" or "NO" to indicate your response.

- If YES, you may want to append the security assessment to this PIA. Go to Question 20.
- If NO, go to Question 19.

17. Are all digital records stored on government servers and are all physical records stored in government offices with government security?

Type "YES" or "NO" to indicate your response.

- If YES, go to Question 20.
- **If NO, describe where the records are stored and the technical and physical security measures in place to protect those records.**

18. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past.

Strategy (EXAMPLES)	
We only allow employees in certain roles access to information	
Employees that need standing or recurring access to personal information must be approved by executive lead	

Strategy (EXAMPLES)	
We use audit logs to see who accesses a file and when	
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6, you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

19. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

20. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

20.1 **Do you have a process in place to correct personal information?**

Type "YES" or "NO" to indicate your response.

20.2 **Sometimes it's not possible to correct the personal information.** *FOIPPA* requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "YES" or "NO" to indicate your response.

20.3 **If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, *FOIPPA* requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?**

Type "YES" or "NO" to indicate your response.

21. Does your initiative use personal information to make decisions that directly affect an individual?

Type "YES" or "NO" to indicate your response.

- If YES, go to Question 24.
- If NO, skip ahead to Part 7.

22. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

Type “YES” or “NO” to indicate your response.

- If NO, describe how you will ensure the information will be kept for a minimum of one year after it’s used to make a decision that directly affects an individual.

PART 7: PERSONAL INFORMATION BANKS

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

23. Will your initiative result in a personal information bank?

Type "YES" or "NO" to indicate your response.

- If YES, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

24. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing, or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Add new rows if necessary.

Possible risk	**Response**
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 9: SIGNATURES

You have completed a Privacy Impact Assessment. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

25. Privacy Officer Comments

26. Privacy Officer Signatures

This PIA is based on a review of the material provided to the Privacy Officer as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Advisor			
Manager or Director Only required if personal information is involved			

27. Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored, or disclosed, the program area will engage with their Privacy Officer and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Program/Department Manager			

Role	Name	Electronic signature	Date signed
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate (if required)			

APPENDIX D

Information Sharing Agreement (ISA) Template

Dated the _____ day of _____, 20___.

BETWEEN:

[First Party]

("Party X")

Agreement Administrator:

Party X

Ph:

Fax:

Email:

AND:

[Other Party]

("Party Y")

Agreement Administrator:

Party Y

Ph:

Fax:

Email:

Add other parties as required.

1. Purpose of this Agreement

The purpose of this Agreement is to document the terms and conditions of the exchange of certain personal information by the Parties, in compliance with the *Freedom of Information and Protection of Privacy Act* and other applicable legislation (if any).

2. Summary of Information Sharing

Describe what program, activity, or initiative the ISA is being drafted to support. This section could also summarize the information sharing and the context in which it takes place.

3. Purpose of the Information Sharing

This section should explain the purpose of the initiative. This description could include its benefits and the larger activity (if any) of which it is a part. Your response may already be found in Question 1 of the Privacy Impact Assessment (PIA) related to this initiative.

4. Personal Information

For the definition of personal information, the CCRD follows the definition provided by the provincial government found here: Personal Information Definitions.

Insert description of information to be covered by the Agreement. If different types of information are to be handled differently under the Agreement, break the definition down accordingly.

5. Collection and Disclosure of Personal Information

Describe the exchange of information under the Agreement. If different types of information are to be collected and/or disclosed differently, break the description down accordingly. For each receiving body that is a public body, state the authority (under sections 26 and 27) for collection. For each disclosing body that is a public body, state the authority (under section 33) for disclosure. If there are other legislative provisions that work together with the *Freedom of Information and Protection of Privacy Act* to provide authority for collection and/or disclosure, state what those provisions are. This information can be found in the Privacy Impact Assessment (PIA) related to this initiative. For any questions, contact the Privacy Officer/Corporate Officer.

6. Use of Personal Information

Describe the use(s) to which each body will put the information and state the authority (under section 32) for those use(s). If there are other legislative provisions that govern the use of the information, state what those provisions are.

7. Accuracy

Each Party will make every reasonable effort to ensure the Personal Information in its custody is accurate, complete and up to date.

8. Security

8.1 Each Party will make reasonable arrangements to maintain the security of the Personal Information in its custody, by protecting it against such risks as unauthorized access, collection, use, disclosure or disposal.

8.2 Each Party will implement this Agreement in conformity with the government's Information Security Policy.

8.3 Each Party will advise the other Party immediately of any circumstances, incidents or events which to its knowledge have jeopardized or may in future jeopardize:

- the privacy of individuals;
- the security of any computer system in its custody that is used to access the Personal Information.

9. Compliance Monitoring and Investigations

9.1 Each party will record and monitor access to the Personal Information in its custody, in order to establish a chain of responsibility, as follows:

Describe compliance monitoring methodology and timetable. Use an appendix to provide more detail, if required. If using an appendix, change "as follows" to "as set out in Appendix "A" to this Agreement".

9.2 Each Party will investigate all reported cases of:

- unauthorized access to or modification of the Personal Information in its custody;
- unauthorized use of the Personal Information in its custody;
- unauthorized disclosure of the Personal Information in its custody;

- breaches of privacy or security with respect to the Personal Information in its custody or with respect to any computer system in its custody that is used to access the Personal Information.

9.3 Each Party will report to the other the results of any such investigation and the steps taken to address any remaining issues or concerns about the security of the Personal Information or computer systems, or the privacy of individuals to whom the Personal Information relates.

10. Modification or Termination of Agreement – General

10.1 This Agreement may be modified or terminated at any time by agreement, in writing, of [both/all] parties.

11. Termination for Non-Compliance with Agreement

11.1 This Agreement may be terminated at any time by either Party if the other Party fails to meet its obligations under this Agreement.

If there are more than two parties, revise paragraph 11.1 as required.

12. Term of Agreement

This Agreement will be in force during the period commencing [Date] and ending [Date] unless sooner terminated in accordance with paragraph 10.1 or paragraph 11.1.

13. Appendices

Any appendices to this Agreement are part of the Agreement. If there is a conflict between a provision in an appendix and any provision of this Agreement, the provision in the appendix is inoperative to the extent of the conflict unless it states that it operates despite a conflicting provision of this Agreement.

If appendices are not used, clause 13 can be deleted.

Agreed to on behalf of Party X:

(Authorized representative) Date

Agreed to on behalf of Party Y:

(Authorized representative) Date