

# PRIVACY IMPACT ASSESSMENT

## I BASIC INFORMATION - New or Existing Program, System or Legislation

### 1. Ministry/Public Body and Program Area.

Ministry	Ministry of Environment
Division	BC Parks and Conservation Officer Service Division
Branch/Section	Conservation Officer Service, Support Services
Initiative Title	ICBC and COS Information Sharing Agreement

### 2. Contact Position and/or Name, Telephone Number and E-Mail Address.

(This should be the name of the individual most qualified to respond to questions regarding the PIA).

Name, Title	Wayne Zimmerman, Inspector,
Branch/Section	Conservation Officer Service, Support Services
Phone Number	(250) 356-6144
E-Mail	Wayne.Zimmerman@gov.bc.ca

### 3. Description of the Program/System/Legislation (Initiative) being assessed.

(Please note here if the initiative does not collect, use or disclose personal information). If this is a change to an existing legislation, system or program, describe the current system or program and the proposed changes.

This PIA assesses access by the Conservation Officer Service (COS) to ICBC database through an Information Sharing Agreement (ISA) for access to personal information relating to vehicle registered owners and driver's licence data.

The British Columbia Conservation Officer Service is a professional law enforcement agency that is a progressive and respected leader in environmental compliance & enforcement, shared stewardship and public safety. Information accessed through the ISA will be used to assist conservation officers with investigations into contraventions of provincial environmental legislation. Sections 106 through 108.1 of the *Environmental Management Act* authorize a conservation officer to exercise and perform the duties of an officer and enforce the prohibitions or requirements under that Act, and other prescribed enactments. Note: PIAs were completed for the collection of personal information in the performance of duties under EMA as well as the Conservation Service Authority Regulation, BC Reg. 318/2004 at the time the legislation was developed.

		*Yes	No
(a)	Does this PIA involve a common or integrated program/activity (as defined in the FOIPP Act)? and		x
	Is the common or integrated program/activity confirmed by the written requirements set out in the regulation?		x
(b)	Does this PIA involve a data-linking initiative (as defined in the FOIPP Act)?		x

If yes, please ensure you have notified the Office of the Information and Privacy Commissioner at an early stage of development of the Initiative pursuant to section 69 (5.5) of the FOIPP Act.

**4. Purpose/Objectives of the initiative (if statutory, provide citation).**

Access to ICBA data through the ISA is sought to retrieve information on persons-of-interest or vehicles-of-interest.

Conservation officers (COs) carry out law enforcement services in rural, wilderness and urban settings by conducting area patrols, road blocks, vessel and vehicle inspections, including business vehicle inspections. In the course of conducting their mandated duties COs often come across individuals in remote areas who are armed or who are transporting loaded firearms in vehicles; they encounter others who are illegally transporting wastes; they often respond to public report/complaints of suspicious activity where a vehicle description and plate number are the only information available; they frequently come across individuals who are involved in a wide range of other criminal activities.

In these instances accurate identity knowledge of the individuals involved, or who they may have to deal with, helps ensure officer safety and efficient coordination within the law enforcement community. Access to the ICBC database will be part of information gathering from multiple sources, internal and external to the Ministry, analyzed to confirm identity and risks.

Additionally, CO's are responsible to verify the accuracy of identifying information prior to use or reliance on the information for further investigation or in preparing evidence for a case to go before the courts.

**5. What are the potential impacts of this proposal? (Include privacy impacts in this description).**

The impacts of this proposal are positive with respect to creating communication efficiency through direct electronic access to the database. Without direct access to this information it is extremely difficult to complete the background investigation necessary to guarantee officer and public safety and to continue investigation of suspected violations.

**6. Provide details of any previous PIA or other form of personal information assessment done on this initiative (in whole or in part).**

No previous assessments have been completed on this initiative.

**IF THERE IS NO PERSONAL INFORMATION INVOLVED, GO TO X. SIGNATURES.**

**\*\*IMPORTANT NOTE:** The FOIPP Act defines personal information as "recorded information about an identifiable individual other than contact information." Contact information includes the name, title, telephone or facsimile number, email address etc., which enables an individual at a place of business to be contacted.

**II DESCRIPTIVE INFORMATION**

**1. Describe the elements of personal information that will be collected, used and/or disclosed and the nature and sensitivity of the personal information. [See note above about the definition of personal information.]**

*For example: Name, home address, gender, age/birthdate, SIN, Employee#, race/national, ethnic origin.*

The personal information that will be accessed and/or collected from the ICBC database via the ISA includes information concerning:

- name,
- birth date,
- home address,
- home phone number,
- driver's license number,

- driver's licence status (e.g. Normal, Hold, Surrendered, Prohibited),
- Registered owner name and address,
- Vehicle description, registration number, and Vehicle Identification Number,
- Vehicle license history, and plate vehicle history.

**2. Provide a description (either a narrative or flow chart) of the linkages and flows of personal information collected, used and/or disclosed.**

**Example #1**

1. Conservation officer encounters a resource user.
2. Resource user supplies personal information/vehicle information to a CO in the form of identification.
3. Conservation officer collects (records) personal information/vehicle information from resource user.
4. Conservation officer accesses ICBC database for verification of provided information.
5. CO opens an investigation file and saves all information in the file, including details on accessing ICBC database.
6. CO conducts investigation and continually updated the investigation file.

**Example #2**

1. Conservation officer receives public report/complaint of suspicious activity including a vehicle description and licence plate number.
2. Conservation officer inspects area of complaint and discovers evidence of an offence.
3. Conservation officer accesses ICBC database to seek verification of vehicle information.
4. Conservation officer accesses ICBC database to conduct further investigation to collect vehicle registered owner information associated to the vehicle reportedly involved in a potential violation.
5. CO opens an investigation File and saves all information in the file including details on accessing ICBC database.
6. CO conducts investigation and continually updates the investigation file.

## III

**PERSONAL INFORMATION COLLECTION**(Section 26 and section 27 of the *Freedom of Information and Protection of Privacy Act* "FOIPP Act")

**\*\*IMPORTANT NOTE:** Recent amendments to the FOIPP Act have clarified when personal information has *not* been collected by a public body. See section 27.1 or contact Knowledge and Information Services for further details.

	Yes	No	n/a
Is personal information being collected?	X		

**IF THERE IS NO PERSONAL INFORMATION BEING COLLECTED, GO TO IV. USE OF PERSONAL INFORMATION**

**1) Authorization for Collection:**

A public body may collect personal information as authorized by one of the following provisions:

s. 26		Yes	No	n/a
(a)	Is the collection of personal information specifically authorized by, or under, an Act, other than the FOIPP Act?		X	
	<b>If yes, please specify the name of the Act and relevant section</b>			
(b)	Is the personal information being collected for law enforcement purposes?	X		
(c)	Is the personal information directly related to, and necessary for, a program or activity of the public body?	X		
(d)	Is the personal information being collected for a prescribed purpose (where there is a regulation defining that purpose)?		X	
	<b>If yes, please specify the prescribed purpose.</b>			
	(i) Has the individual whose personal information is being collected consented, in the prescribed manner, to that collection?			
	and			
	(ii) Would a reasonable person consider that collection appropriate in the circumstances?			
(e)	Is the collection of personal information necessary for the purposes of planning or evaluating a program or activity of a public body?		X	
(f)	Is the collection of personal information necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur?		X	
(g)	Is the personal information being collected by observation at a presentation, ceremony, performance, sports meet, or similar event where the individual voluntarily appears and that is open to the public? <b>Please identify event:</b>		X	
(h)	Is personal identity information being collected by:			

s. 26		Yes	No	n/a
	A designated provincial identity information services provider and the collection of the information is necessary to enable it to provide services under section 69.2, or		X	
	A public body from a designated provincial identity information services provider and the collection of the information is necessary to enable the public body to identify an individual for the purposes of providing a service to the individual or the provincial identity information services provider to provide services under section 69.2.		X	

If none of the above questions has been answered "yes", your office does not have the authority under the FOIPP Act to collect the personal information in question. If you have any questions or require clarification please contact Knowledge and Information Services.

## 2) How will the personal information be collected?

A public body must collect personal information directly from the individual the information is about, with certain specific exceptions.

	Yes	No	n/a
Will the personal information be collected <u>directly</u> from the individual that the information is about?	X	X	
<i>*Personal Information may be collected directly from the individual in the form of names, address, date of birth and other vehicle related information, during routine compliance or enforcement checks. Personal information will be indirectly collected through the ISA to help verify collected information or fill information gaps to help complete investigation information and determine officer and public safety risks. There may be instances during covert operations that the individual would not be aware of the collection of information.</i>			

**IF YOU ARE ONLY COLLECTING PERSONAL INFORMATION DIRECTLY AS NOTED ABOVE, YOU WILL NOT NEED TO COMPLETE THE NEXT SECTION ON INDIRECT COLLECTION. GO TO 3. NOTIFICATION TO COLLECT INFORMATION.**

If the personal information has **not been collected directly** from the individual it is about, check which of the following authorizes the indirect collection:

s. 27(1)		Yes	No	n/a
(a)(i)	Did the individual the information is about authorize another method of collection?		X	
(a)(ii)	Has indirect collection been authorized by the Information and Privacy Commissioner?		X	
(a)(iii)	Has indirect collection been authorized by another enactment?		X	
	<b>If yes, please specify the name of the Act and relevant section(s)</b>			
(a.1)(i)	Is the personal information necessary for the medical treatment of an individual and it is not possible to collect the information directly from that individual?		X	

s. 27(1)		Yes	No	n/a
(a.1)(ii)	Is the personal information necessary for the medical treatment of an individual and it is not possible to obtain authority under (iv) for another method of collection?		X	
(b)	Is the public body collecting personal information disclosed to it by another public body under an authority within sections 33 to 36 of the FOIPP Act?	X		
	<b>Specify relevant section(s) or subsections that apply.</b> S. 33.1 (1) (k) (ii) s. 33.2 (i)			
(c)(i)	Is the personal information being collected for the purpose of determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary?		X	
(c)(ii)	Is the personal information being collected for the purpose of a proceeding before a court or a judicial or quasi-judicial tribunal?		X	
(c)(iii)	Is the personal information being collected for the purpose of collecting a debt or fine or making a payment?		X	
(c)(iv)	Is the personal information being collected for the purpose of law enforcement?	X		
(c)(v)	Is the personal information being collected to reduce the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur?			X
(d)	Is the personal information being transferred to the public body from another public body in accordance with section 27.1?		X	
(e)	Is the personal information being collected necessary for delivering a common or integrated program or activity?		X	
(f)	Is the personal information about an employee, other than a service provider, and the collection of the information is necessary for the purposes of managing or terminating an employment relationship between a public body and the employee?		X	
(g)	Is the information personal identity information that is collected by the designated provincial identity information service that is necessary to provide services under section 69.2?		X	
	<b>Additional details as required (e.g., explanation of method of collection)</b>			

***If none of the above authorities have been checked, your office does not have the authority under the FOIPP Act to collect the personal information in question. If you have any questions or require clarification please contact Knowledge and Information Services.***

### **3) Notification to collect information**

A public body must ensure that an individual from whom it collects personal information is notified of the collection as outlined below.

27(2)		Yes	No	n/a
	Has the individual from whom personal information is being collected, been informed of:			
	(a) the purpose for collection?		X	
	(b) the legal authority for collection?		X	
	(c) the contact information of the person who can answer questions regarding the collection?		X	
	<b>Additional details as required (e.g., method of notification)</b>			

**Notification is not required if the answer is "yes" to any of the following:**

27(3)		Yes	No	n/a
(a)	Is the personal information about law enforcement or anything referred to in section 15(1) or section 15(2) of the FOIPP Act?	X		
(b)	Has the Minister responsible for the FOIPP Act excused your public body from complying because it would			
	(a) result in the collection of inaccurate information?		X	
	<b>or</b>			
	(b) defeat the purpose or prejudice the use for which the personal information is collected?		X	
(c)	The information			
	(a) is not required, under subsection 27(1), to be collected directly from the individual the information is about, <b>and</b>	X		
	(b) is not collected directly from the individual the information is about			
(d)	Is the information collected by observation at a presentation, ceremony, performance, sports meet or similar event at which the individual voluntarily appears and that is open to the public.		X	
	<b>Please identify event:</b>			
27 (4)	Is it reasonable to expect that notifying an employee of collection under subsection 27 (1) (f) would compromise			
	(a) the availability or accuracy of the information, or		X	
	(b) an investigation or a proceeding related to the employment of the employee?			
	<b>Additional details as required</b>			
	The information is collected for Law Enforcement purposes ONLY.			

***If you have not provided the required notification as outlined above, please contact Knowledge and Information Services.***

**IV USE OF PERSONAL INFORMATION - (Section 32 of the FOIPP Act)**

	Yes	No	n/a
Is personal information being used?	X		

**IF THERE IS NO PERSONAL INFORMATION BEING USED, GO TO V. DISCLOSURE OF PERSONAL INFORMATION**

*Under the FOIPP Act, a public body may use personal information in its custody or under its control only for certain specified purposes as outlined below.*

The public body **must** check one or more of the authorities listed below:

s.32		Yes	No	n/a
(a)	Has the individual the personal information is about consented to the use? (Note: Supporting documentation must be on file.)		X	
(b)	Will the information be used only for the purpose for which it was obtained or compiled or for a use consistent with the original purposes?	X		
	<b>Please provide details of the original purpose for which the personal information was obtained or compiled. Include, if applicable, details of the consistent/secondary use.</b>  CONSISTENT USE – to confirm/verify individual and vehicle identification, and assist in specific COS investigations.			
(c)	If the personal information was disclosed to the public body by another public body under an authority within sections 33 to 36, is the information being used for that same purpose?	X		
	<b>Specify subsection(s) being applied</b> 33.1(1)(k)(ii) and 33.2(i)			

*If you have not checked one of the above, you do not have the authority to use the information. If you have any questions or require clarification please contact Knowledge and Information Services.*

**V DISCLOSURE OF PERSONAL INFORMATION**

(Section 33, section 33.1, section 33.2, section 33.3, section 34, section 35 and section 36 of the FOIPP Act)

	Yes	No	n/a
Is personal information being disclosed?	X		

**IF THERE IS NO PERSONAL INFORMATION BEING DISCLOSED, GO TO VI. ACCURACY AND CORRECTION OF PERSONAL INFORMATION.**

*A public body may disclose personal information in its custody or under its control only as permitted under sections 33.1, 33.2, or 33.3 of the FOIPP Act.*

**1) Disclosure of Personal Information**



Sections 33, 33.1, 33.2 and 33.3 of the FOIPP Act provide the legislative authority to disclose personal information. Section 33 provides that personal information **cannot** be disclosed unless it is authorized under section 33.1 or 33.2.

Please choose the main authorization(s) for disclosure below. All authorities that may apply do not need to be checked, only the main authorizations for the Initiative.

s. 33.1	Disclosure inside OR outside Canada	Yes	No	n/a
(1)(a)	In accordance with Part 2 (pursuant to an FOI request)		X	
(1)(a.1)	If the information or disclosure is of a type described in section 22(4) (e), (f), (h), (i) or (j):  22(4) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if			
	(e) the information is about the third party's position, functions or remuneration as an officer, employee or member of a public body or as a member of a minister's staff,		X	
	(f) the disclosure reveals financial and other details of a contract to supply goods or services to a public body,		X	
	(h) the information is about expenses incurred by the third party while travelling at the expense of a public body,		X	
	(i) the disclosure reveals details of a licence, permit or other similar discretionary benefit granted to the third party by a public body, not including personal information supplied in support of the application for the benefit, or		X	
	(j) the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body, not including personal information that is supplied in support of the application for the benefit or is referred to in subsection 22(3)(c).		X	
(1)(b)	If the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable (Note: Supporting documentation must be on file)		X	
(1)(c)	In accordance with an enactment of British Columbia (other than the <i>Freedom of Information and Protection of Privacy Act</i> ) or Canada that authorizes or requires its disclosure		X	
	<b>Specify name of enactment and relevant section(s)</b>			
(1)(c.1)	If the personal information is made available to the public in British Columbia under an enactment, (other than the <i>Freedom of Information and Protection of Privacy Act</i> ) that authorizes or requires the information to be made public		X	
	<b>Specify name of enactment and relevant section(s)</b>			

s. 33.1	Disclosure inside OR outside Canada	Yes	No	n/a
(1)(d)	In accordance with a provision of a treaty, arrangement or written agreement that (i) authorizes or requires its disclosure, and (ii) is made under an enactment of British Columbia (other than the <i>Freedom of Information and Protection of Privacy Act</i> ) or Canada		X	
	<b>Specify name of enactment and relevant section(s)</b>			
(1)(e)	To an individual who is a minister, an officer of the public body or an employee of the public body other than a service provider, if (i) the information is necessary for the performance of the duties of the minister, officer or employee,		X	
	<b>and</b> (ii) in relation to disclosure outside Canada, the outside disclosure is necessary because the individual is temporarily travelling outside Canada			
	<b>If paragraph (1)(e)(ii) applies, please explain how the travel is temporary and why disclosure outside Canada is necessary</b>			
(1)(e.1)	To an individual who is a service provider of the public body, or an employee or associate of such a service provider, if (i) the information is necessary for the performance of the duties of the individual in relation to the public body,		X	
	<b>and</b> (ii) in relation to disclosure outside Canada, (A) the individual normally receives such disclosure only inside Canada for the purpose of performing those duties, and (B) the outside disclosure is necessary because the individual is temporarily travelling outside Canada			
	<b>If paragraph (1)(e.1)(ii) applies, please explain how the travel is temporary and why disclosure outside Canada is necessary</b>			
(1)(f)	To an officer or employee of the public body or to a minister, if the information is immediately necessary for the protection of the health or safety of the officer, employee, or minister		X	
(1)(g)	To the Attorney General or legal counsel for the public body, for the purpose of preparing or obtaining legal advice for the government or public body or for use in civil proceedings involving the government or public body		X	
(1)(h)	To the minister responsible for the <i>Coroner's Act</i> or a person referred to in section 36 of that Act, for the purposes of that Act		X	
(1)(i)	If			
	(i) the disclosure is for the purposes of collecting amounts owing to the government of British Columbia or a public body by		X	
	a. an individual, or			

	b. corporation of which the individual the information is about is or was a director or officer,			
	<b>and</b>			
	(ii) in relation to disclosure outside Canada, there are reasonable grounds for believing that			
	a. the individual the information is about is in, resides in or has assets in the other jurisdiction, or			
	b. if applicable, the corporation was incorporated in, is doing business in or has assets in the other jurisdiction			
<b>1(l.1)</b>	For the purposes of			
	(i) a payment to be made to or by the government of British Columbia or a public body,		X	
	(ii) authorizing, administering, processing, verifying or cancelling such a payment, or		X	
	(iii) resolving an issue regarding such a payment		X	
<b>(1)(j)</b>	(i) Repealed.			
<b>(1)(k)</b>	For the purposes of			
	(i) licensing or registration of motor vehicles or drivers, or		X	
	(ii) verification of motor vehicle insurance, motor vehicle registration or drivers licences	X		

<b>(1)(l)</b>	For the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada by governing bodies of professions and occupations		X	
<b>(1)(m)</b>	If			
	(i) the head of the public body determines that compelling circumstances exist that affect anyone's health or safety, and		X	
	(ii) notice of disclosure is mailed to the last known address of the individual the information is about, unless the head of the public body considers that giving this notice could harm someone's health or safety			
<b>(1) (m.1)</b>	For the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur		X	
<b>(1)(n)</b>	So that the next of kin or a friend of an injured, ill or deceased individual may be contacted		X	
<b>(1)(o)</b>	In accordance with section 36 (disclosure for archival or historical purposes)		X	
<b>(1)(p)</b>	The disclosure			
	(i) is necessary for			
	(A) installing, implementing, maintaining, repairing, trouble shooting or upgrading an electronic system or equipment that includes an electronic system that is used in Canada by the public body or by a service provider for the purposes of providing services to a public body, or		X	

	(B) data recovery that is being undertaken following failure of an electronic system that is used in Canada by the public body or by a service provider for the purposes of providing services to a public body			
	<b>and</b> (ii) in the case of disclosure outside Canada (A) is limited to temporary access and storage for the minimum time necessary for that purpose, and (B) in relation to data recovery under subparagraph (i)(B), is limited to access and storage only after the system failure has occurred			
	<b>If paragraph (1)(p)(ii) applies, please explain how the temporary access and storage is for the <i>minimum time necessary</i></b>			
(1)(q)	If the information was collected by observation at a presentation, ceremony, performance, sports meet or similar event at which the individual voluntarily appeared and that was open to the public. <b>Please identify event:</b>		X	
(1)(r)	If the information Was disclosed on a social media site by the individual the information is about,		X	
	Was obtained or compiled by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion respecting proposed or existing initiatives, policies, proposals, programs or activities of the public body or respecting legislation relating to the public body, <b>and</b>			
	Is disclosed for a use that is consistent with the purpose described in subparagraph (ii).			
	<b>Additional details as required</b>			
(1)(s)	In accordance with section 35 (disclosure for research or statistical purposes).		X	
(1)(t)	To comply with a subpoena, a warrant or an order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information		X	
(2)	In addition to the authority under any other provision of this section or section 33.2, a public body that is a law enforcement agency may disclose personal information referred to in section 33			
(2)(a)	To another law enforcement agency in Canada		X	
(2)(b)	To a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority.		X	

(3)	The minister responsible for this Act may, by order, allow disclosure outside Canada under a provision of section 33.2 in specific cases or specified circumstances, subject to any restrictions or conditions that the minister considers advisable.		X	
(4)	In addition to the authority under any other provision of this section or section 33.2, the Insurance Corporation of British Columbia may disclose personal information if,  (a) the information was obtained or compiled by that public body for the purposes of insurance provided by the public body, and  (b) disclosure of the information is necessary to investigate, manage or settle a specific insurance claim.		X	
(5) and (6)	For the purposes of operating the designated provincial identity information services as permitted under section 33.1 (5) and (6)		X	
(7)	To respond to citizens' enquiries as permitted under section 33.1(7)		X	
	<b>Additional details as required</b>			

s. 33.2	Disclosure inside Canada only	Yes	No	n/a
(a)	For the purpose for which it was obtained or compiled or for a use consistent with that purpose (see section 34)	X		
	<b>Please provide details of the original purpose for which the personal information was obtained or compiled. Include, if applicable, details of the consistent/secondary use.</b>  To confirm/verify individual and vehicle identification, and assist in specific COS investigations.			
(b)	Repealed.			
(c)	To an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister		X	
(d)	To an officer or employee of (i) a public body, or (ii) an agency  or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties, respecting the common or integrated program or activity, of the officer, employee or minister to whom the information is disclosed		X	
(e)	To an officer or employee of a public body or to a minister, if the information is necessary for the protection of the health or safety of the officer, employee or minister		X	
(f)	To the auditor general or any other prescribed person or body for audit purposes		X	
(g)	To a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem		X	

<b>s. 33.2</b>	<b>Disclosure inside Canada only</b>	<b>Yes</b>	<b>No</b>	<b>n/a</b>
<b>(h)</b>	To a representative of the bargaining agent, who has been authorized in writing by the employee whom the information is about, to make an inquiry		X	
<b>(i)</b>	To a public body or a law enforcement agency in Canada to assist in a specific investigation			
	(i) undertaken with a view to a law enforcement proceeding, or	X		
	(ii) from which a law enforcement proceeding is likely to result	X		
<b>(j)</b>	To the archives of the government of British Columbia or the archives of a public body, for archival purposes		X	
<b>(k)</b>	Repealed.			
<b>(l)</b>	To an officer or employee of a public body or to a minister, if the information is necessary for the purposes of planning or evaluating a program or activity of a public body		X	
	<b>Additional details as required</b>			

<b>s. 33.3</b>	<b>Disclosure to Public Without Request</b>	<b>Yes</b>	<b>No</b>	<b>n/a</b>
<b>(1)</b>	Do the records fall within a category established under section 71 (1)?		X	
	<b>Additional details as required</b>			
<b>(2)</b>	Do the records fall within a category established under section 71.1 (1)?		X	
	<b>Additional details as required</b>			

**2) Systematic or Repetitious Disclosure/Exchanges?**

		<b>Yes</b>	<b>No</b>	<b>n/a</b>
<b>i.</b>	Do the disclosures of personal information under section 33.2 occur on a regular basis?	X		
<b>ii.</b>	Has an Information Sharing Agreement been completed for these disclosures/exchanges?		X	
	<i>* An ISA is being completed based on the authorities identified in this PIA.</i>			
<b>iii.</b>	Has information related to the Information Sharing Agreement(s) been entered into the Personal Information Directory?		X	

**Personal information exchanges within a public body do not normally require an Information Sharing Agreement (ISA) if they are for a consistent purpose as defined under section 33.2(a) of the Act or are necessary for the performance of an employee of the public body under section 33.2(c). However, depending on the nature and sensitivity of the personal information exchanged, the public body might choose to prepare an ISA or similar written statement of understanding.**

3) **Research or Statistical Purposes (Section 35)**

	Yes	No	n/a
Has a researcher requested access to personal information in an identifiable form for research purposes?		X	

If "yes", a research agreement that conforms to the criteria established in section 35(d) must be in place. Contact Knowledge and Information Services for assistance.

**Please note:** Research using personal information may only be conducted if it meets all of the terms of section 35.

4) **Archival or Historical Purposes (Section 36)**

The archives of the government of British Columbia, the archives of a public body, or a board or a francophone education authority (as defined in the *School Act*) may disclose personal information in its custody or under its control to be disclosed for archival or historical purposes as authorized by section 36.

Please check the authorization(s) for disclosure listed below.

		Yes	No	n/a
(a)	The disclosure would not be an unreasonable invasion of personal privacy under section 22		X	
(b)	The disclosure is for historical research and is in accordance with section 35 (research agreements)		X	
(c)	The information is about someone who has been dead for 20 or more years		X	
(d)	The information is in a record that has been in existence for 100 or more years		X	

***If you have not answered "yes" to any of the above authorizations for disclosure you do not have the authority to disclose personal information. If you have any questions or require clarification, please contact Knowledge and Information Services.***

**VI ACCURACY AND CORRECTION OF PERSONAL INFORMATION**  
(Section 28 and section 29 of the FOIPP Act)

If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must make every reasonable effort to ensure that the information is accurate and complete. An individual must also have the ability to access, or have corrected or annotated, their personal information for a period of one year after a decision has been made based upon the personal information.

		Yes	No	n/a
1.	Are there procedures in place to enable an individual to request/review a copy of their own personal information?	X		
2.	Are there procedures in place to correct or annotate an individual's personal information if requested, including what source was used to update the file?	X		

3.	If personal information is corrected, are there procedures in place to notify other holders of this information?		X		
If yes, please provide the name of the policy and/or procedures, a contact person and phone number.					
	Policy/procedure:	Section 29 of FOIPPA			
	Contact person:	Information Access Operations			
	Phone number:	250-387-1321			
Additional details as required					

*If any of the questions above have been answered "no", please contact Knowledge and Information Services for further clarification.*

## VII SECURITY AND STORAGE FOR THE PROTECTION OF PERSONAL INFORMATION (Sections 30 and 30.1 of the FOIPPA Act)

**Note:** For PIAs related to new or existing systems, this section should be completed by the Branch of the ministry responsible for systems maintenance and security, and signed off by this branch, in the Signatures section.

For PIAs that do not involve systems initiatives, this section should be completed by the program area completing the PIA. In this case, the signature of the systems representative is not required.

Section 30 of the Act requires a public body to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

		Yes	No	n/a
1.	Is there reasonable technical security in place to protect against unauthorized access or disclosure?	X		
2.	Is there reasonable physical security in place to protect against unauthorized access or disclosure?	X		
3.	Are there branch policies and procedures in place for the security of personal information during routine collection, use and disclosure of the information?	X		
If yes, please provide the name of the policy and/or procedures, a contact person and phone number.				
	Policy/procedure:	Information Security Policy		
	Contact person:	Nick Corcoran		
	Phone number:	250-356-2825		



	<b>Additional details as required</b>			
	As part the public service, COs are accountable to protect personal information privacy as described in the <i>Freedom of Information and Protection of Privacy Act</i> (the Act) and must comply with the provisions of the Act and its regulation as well as being governed by Government's Core Policy and Procedures manual, Information Management and Information Technology Management.			
	In addition, COS program policy and procedure on Code of Professional Conduct addresses improper disclosure of information.			
4.	Have user access profiles been assigned on a need-to-know basis?	X		
5.	Do controls and procedures exist for the authority to add, change or delete personal information?	X		
6.	Does your system security include an ongoing audit process that can track use of the system (e.g., when and who accessed and updated the system)?		X	
	<b>Please explain the audit process and indicate how frequently audits are undertaken and under what circumstances</b>			
7.	Does the audit identify inappropriate accesses to the system?		X	
	<b>Additional details</b>			

*If any of the questions above have been answered "no", please contact your Ministry's Security Officer. If you have any questions or require clarification please contact Knowledge and Information Services.*

## VII SECURITY ARRANGEMENTS FOR THE PROTECTION OF PERSONAL INFORMATION cont'd

Section 30.1 requires a public body to ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada unless the individual the information is about has consented or the disclosure is otherwise allowable under the Act.

	Yes	No	n/a
Will the information be stored or accessed only in Canada?	X		

**Personal information in a public body's custody or under its control must be stored and accessed only in Canada, unless one of the following applies:**

	Yes	No	n/a
(a) Has the individual the personal information is about identified it and consented, in the prescribed manner, to it being stored in or accessed from another jurisdiction?		X	
<b>Please explain</b>			

(b)	Will the personal information be stored in or accessed from another jurisdiction for the purpose of a disclosure that is authorized under the <i>Freedom of Information and Protection of Privacy Act</i> ?		X	
	Please explain			
(c)	Will the personal information be disclosed under section 33.1(1)(i.1)?		X	
	Please explain			

*If you have not answered "yes" to any of the above authorizations for storage or access of personal information outside Canada or if you require clarification, please contact Knowledge and Information Services.*

## VIII RETENTION OF PERSONAL INFORMATION - (Section 31 of the FOIPP Act)

**If a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.**

		Yes	No	n/a
1.	Do you have an approved records retention and disposition schedule?		X	
	*COS is currently using a draft ORCS			
2.	Is there a records retention schedule to ensure information used to make a decision that directly affects an individual is retained for at least one year after use?	X		

*If you answered "no" to the above questions, your procedures may need to be revised. Please contact your Records Officer.*

**Note:** Records of provincial public bodies and designated organizations/public bodies cannot be destroyed unless approval is granted under the authority of the *Document Disposal Act*. Please consult with your Records Officer to initiate the records scheduling process.

**Comments:**

1. 1/1/11

2. 1/1/11

3. 1/1/11

4. 1/1/11

5. 1/1/11

6. 1/1/11

X SIGNATURES

PUBLIC BODY APPROVAL:

Kelly Larkin, Chief Conservation Officer  
Ministry of Environment



Signature

2013-08-15

Date

Eileen Carlson  
Legislation, Privacy and Policy Branch  
Office of the Chief Information Officer  
Ministry of Technology, Innovation and  
Citizens' Services

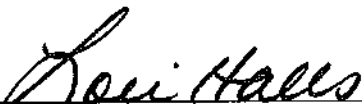


Signature

Aug 21, 2013

Date

Lori Halls  
Assistant Deputy Minister or Equivalent



Signature

Sept. 16/13

Date



## GENERAL ORDERS PART II ORDER #19-2014

<b>Issue Date:</b> August 13, 2014	<b>Effective Date:</b> August 13, 2014	<b>Policy Chapter:</b> Information Management
<b>Subject:</b> ICBC Database		

### Summary

Operational members of Provincial Operations and the Major Investigations Unit have been provided **direct** electronic access to ICBC's database for driver licensing and vehicle registration information.

A recently signed Disclosure of Personal Information Agreement ("Agreement") between the COS and ICBC applies to all personal information disclosed by ICBC to an officer and establishes clear standards for how the information must be managed. The Agreement covers all methods for disclosure, including

- direct electronic access by means of an officer's workstation or tablet;
- access via RCMP or municipal police Operational Communication Centres, in accordance with the terms of separate agreements with those agencies; and
- ICBC's police-only support line.

### Key Provisions of the Agreement

Personal information disclosed by ICBC **must** be managed in accordance with

- COS Policy, Collecting or Disclosing Personal Information, and the
- Disclosure of Personal Information Agreement between the COS and ICBC.

Any failure to comply with the Agreement may result in its termination or a suspension of access and/or the imposition of more restrictive terms and conditions by ICBC.

In particular, officers should take note of the following key provisions from the Agreement:

#### Personal Information to be Disclosed

ICBC will disclose only the following personal information (section 4):

- driver name, birth date, address, driver's license number and driver's licence status;
- registered owner name and address;
- vehicle description, registration number, and Vehicle Identification Number; and
- vehicle license history and plate vehicle history.

Authorized Purposes

Personal information disclosed by ICBC may only be used to (section 6):

- determine ownership of vehicles associated to or believed to be associated to individuals under investigation;
- determine the identity of individuals under investigation;
- identify individuals, and vehicles associated to those individuals, who have criminal backgrounds or who pose a risk to others to ensure officer and public safety;
- assist in the identification of individuals who have been victims or who may be at risk of attacks by wild predatory animals;
- determine the ownership of vehicles which may be associated to individuals being sought by police; and
- determine the ownership of vehicles abandoned on Crown lands.

Records

In accordance with section 5.2 of COS Policy, Collecting or Disclosing Personal Information, and section 7 of the Agreement, an officer who views or collects personal information from the ICBC database must

- record the time and date that access was made and the authorized purpose for which access was required, including any associated file number(s);
- ensure access to the search results is limited to COS staff having a legitimate operational need; and
- maintain each such record for at least two years.

Disclosure by Officer

Personal information may not be disclosed by an officer unless the disclosure complies with the requirements in section 10. While disclosure to a third party is permitted in certain circumstances, the exception provided in section 10.1(d) is **not** to be used as a substitution for another agency obtaining direct access to the ICBC database by means of their own information sharing agreement with ICBC.

**Action Required***Officer*

1. Ensure you are familiar with the requirements and restrictions concerning the use and management of personal information in
  - a. the Disclosure of Personal Information Agreement between the COS and ICBC; and
  - b. COS Policy, Collecting or Disclosing Personal Information.

Note: The Agreement is posted on the COS SharePoint at: Important Links > Agreements and MOUs > ICBC.

2. If practicable, participate in a scheduled online training session on how to access information in the ICBC database (meeting request to follow - Monday, August 18<sup>th</sup>):
  - a. August 20<sup>th</sup>, 9:00am – 10:30am, or
  - b. August 22<sup>nd</sup>, 9:00am – 10:30am.

Note: You will require your driver's licence number and the licence plate number of your work or personal vehicle for this training.

3. If unable to participate in the online training, review the ICBC training materials posted on the COS SharePoint at: Trainer's Corner > ICBC Database. These materials will be made available after the first online session.
4. The software needed to securely access the ICBC database has been installed on your workstation or tablet (i.e. "Attachmate" and "Extra!Session"). You will be provided an ICBC user ID and temporary password, as well as a BC OnLine user ID and password, by Suzanne Tyler, Information Management Branch, prior to online training. Do **not**
  - a. attempt to log-in to either system without first completing the online training or reviewing the training materials; or
  - b. use access to BC OnLine to conduct a search other than a search of the ICBC database.

**Support**

If you require a password reset, contact the ICBC Helpdesk ("Resource Access Control Facility") at: (604) 661-6234.

For technical assistance with using the ICBC database, contact D/Sgt. Dave Hall.

<p><b>Approval:</b> Aaron Canuel, Superintendent Program Support</p>
--



## POLICY AND PROCEDURE CONSERVATION OFFICER SERVICE

---

<b>Title:</b>	Collecting or Disclosing Personal Information
<b>Effective:</b>	July 25, 2014
<b>Revised:</b>	December 16, 2014
<b>Staff Affected</b>	<ul style="list-style-type: none"><li>• Members of the Conservation Officer Service</li><li>• Support Services</li></ul>

---

### CONTENTS

<b>1.0</b>	<b>Purpose.....</b>	<b>2</b>
<b>2.0</b>	<b>References .....</b>	<b>2</b>
<b>3.0</b>	<b>Definitions.....</b>	<b>2</b>
<b>4.0</b>	<b>General Provisions.....</b>	<b>3</b>
4.1	Collecting and Using Personal Information.....	3
4.2	Disclosing Personal Information by COS.....	5
4.3	Confidentiality .....	5
4.4	Information Security .....	6
<b>5.0</b>	<b>Procedure.....</b>	<b>6</b>
5.1	Requesting Disclosure of Personal Information.....	6
5.2	Recording and Documenting.....	6
5.3	Security.....	7



## **1.0 PURPOSE**

1. To provide guidance to Conservation Officer Service (“COS”) staff on their responsibilities and authorities when collecting, using, disclosing and securing personal information to ensure compliance with legislation related to privacy and/or access to personal information.

## **2.0 REFERENCES**

1. *Freedom of Information and Protection of Privacy Act* (“FOIPPA”)
2. *Personal Information Protection Act* (“PIPA”)
3. *Privacy Act* (Canada)
4. Ministry of Finance - Core Policy and Procedures Manual – c 12. 0, Information Management and Information Technology Management
5. Information Security Policy, Office of the Government Chief Information Officer
6. Disclosure of Personal Information Agreement between the COS and ICBC
7. COS Policy 2.2.04, Code of Professional Conduct
8. COS Business Rules for the Notebook

## **3.0 DEFINITIONS**

For the sake of clarity, the following definitions from FOIPPA are included:

1. **Personal information** means recorded information about an identifiable individual other than contact information.
2. **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.
3. **Law enforcement** means
  - a. policing, including criminal intelligence operations;
  - b. investigations that lead or could lead to a penalty or sanction being imposed; or
  - c. proceedings that lead or could lead to a penalty or sanction being imposed.

4. **Public body** means

- a. a ministry of the government of BC;
- b. an agency, board, commission, corporation, office or other body designated in, or added by regulation to Schedule 2 of FOIPPA; 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.

## **4.0 GENERAL PROVISIONS**

### **4.1 Collecting and Using Personal Information**

1. A conservation officer ("officer") shall not collect or use any personal information unless it is necessary to carry out their official duties and the collection or use is authorized under FOIPPA.
2. Two frequently utilized provisions of FOIPPA that authorize an officer to collect personal information, are:
  - a. section 26(b), where the information is collected for the purposes of law enforcement, or
  - b. section 26(c), where the information relates directly to and is necessary for an activity or program of the public body.

Note: An officer who is uncertain of their authority for collecting personal information in a specific circumstance should discuss the situation with their supervisor.

3. FOIPPA requires that personal information be collected directly from the person the information is about. However, section 27(1) exempts this requirement if the personal information is collected for the purposes of law enforcement.
4. Indirect collection of personal information for the purposes of law enforcement may be possible through disclosure of personal information by another public body having custody and control of the information. Provisions of FOIPPA that are commonly used to authorize such disclosure by a public body are:
  - a. section 33.1(1)(d), under an arrangement or written agreement with the specific public body that authorizes or requires information disclosure (e.g. ICBC);
  - b. section 33.1(2)(a), to another law enforcement agency in Canada;
  - c. section 33.2 (a), for a use which is consistent with the purpose for which it was collected;
  - d. section 33.2 (c), if the information is necessary for the performance of the duties of an officer or employee of the public body; or
  - e. section 33.2 (i), to assist in a specific investigation undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result.

Note: Disclosure of CPIC information to the COS occurs under an agreement pursuant to a provision of the *Privacy Act* (Canada), similar to s. 33.1(1)(d) of FOIPPA.

5. Generally, a person must be notified if their personal information is being collected. However, FOIPPA section 27(3)(a) exempts from the requirement for the individual to be told about the purpose and authority for collecting the information, and relevant contact details, if the information is about law enforcement.
6. Federal agencies do not fall under the auspices of FOIPPA. However, certain provisions of the *Privacy Act* (Canada) permit disclosure of personal information under the control of the federal government. For example, under section 8(2)(f) personal information may be disclosed to a provincial institution in BC under agreement for the purpose of administering or enforcing any law or carrying out a lawful investigation. For example, under the Department of Justice - Disclosure of Personal Information Agreement this provision can be utilized for verification of Indian status using the Permissible Disclosure Request Form.
7. Personal information held by organizations in BC (not public bodies) is governed by PIPA. Generally, organizations may only disclose personal information with the consent of the individual. However section 18 contains provisions for disclosure without consent in certain circumstances. Of particular interest to CO's are:
  - a. section 18(c), it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for purposes related to an investigation or a proceeding;
  - b. section 18(i), the disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of personal information; and
  - c. section 18(j), the disclosure is to a public body or a law enforcement agency in Canada, concerning an offence under the laws of Canada or a province, to assist in an investigation, or in the making of a decision to undertake an investigation,
    - i. to determine whether the offence has taken place, or
    - ii. to prepare for the laying of a charge or the prosecution of the offence.
8. As with FOIPPA, PIPA disclosure provisions are permissive and organizations are not compelled to disclose personal information under their control other than to comply with a subpoena or warrant. An officer should discuss any uncertainty with their supervisor, case by case.

#### 4.2 Disclosing Personal Information by COS

1. An officer shall not disclose any personal information unless it is necessary to carry out their official duties and the disclosure is authorized under FOIPPA.
2. Provisions of FOIPPA that may authorize disclosure of personal information held by an officer by reason of his/her employment, include:
  - a. section 33.1(1)(b), with consent of the individual the information is about, as prescribed (see Consent Form);
  - b. section 33.1(1)(c), in accordance with an enactment of BC, other than FOIPPA, or Canada that authorizes or requires its disclosure (e.g. s. 22(5) *Civil Forfeiture Act* which authorizes disclosure to the CFO);
  - c. section 33.1(1)(d), in accordance with an information sharing agreement that is made under an enactment;
  - d. section 33.2(a), for a purpose/use consistent with the reason it was obtained, but only within Canada; or
  - e. section 33.2(i), for law enforcement purposes (allows COS to disclose to another law enforcement agency within Canada only).

Note: FOIPPA authority is permissive, meaning you can release the information if you want to but there is no absolute requirement to do so. However, there are other enactments which may compel the release of the information, including an FOI request. An officer should discuss with their supervisor if uncertain about the authority to disclose personal information.

#### 4.3 Confidentiality

1. All officers commit to apply the highest standard of conduct related to confidentiality, demonstrated by:
  - a. swearing an oath of employment to abide by the Standards of Conduct for Public Service Employees, including the commitment to safeguard confidential information by not divulging it unless either authorized to do so or required to do so by law;
  - b. signing a willingness statement to abide by the COS procedure *Code of Professional Conduct* (and other operational policy and procedures);
  - c. signing an Information and Communications Technology Agreement related to information management, use of technology and personal information protection (Chapter 12, Core Policy and Procedures Manual);
  - d. swearing a police oath under s. 70 of the *Police Act* related to faithfully, honestly and impartially performing their duties as a Special Provincial Constable; and
  - e. completing mandatory privacy training for the public service (IM 111: Information Sharing and Privacy Awareness Training for Employees).
2. Should uncertainty arise about authority for an officer to collect, use or disclose personal information, or whether certain information is confidential, those questions or concerns may be directed through the officer's supervisor to the Inspector, Support Services.
3. Officer behaviour which is contrary to information security policy and procedure is a disciplinary default under the COS *Code of Professional Conduct* and the officer may be subject to corrective measures and/or disciplinary action, including dismissal.

#### 4.4 Information Security

1. The COS must comply with provincial and federal statutory requirements for security safeguards to protect personal information against such risks as unauthorized access, collection, use, disclosure or disposal (e.g. s. 30 FOIPPA).
2. It is the responsibility of all staff to be aware of the government's Information Security Policy and, depending on the source and agreement protocol for access to personal information, any additional specific procedures, conditions or requirements (e.g. CPIC policy, MOU with ICBC, Core P&P Manual for IT and IM, FOIPPA).

### 5.0 PROCEDURE

#### 5.1 Requesting Disclosure of Personal Information

1. If you are seeking disclosure of personal information in the custody or under the control of a public body, and you do not have direct access to the information under the terms of an information sharing agreement, submit a written request on the other agency's / organization's information request form, if available, or use the COS Personal Information Request Form.

Note: Officers should reference the section(s) of FOIPPA which authorize the disclosure of personal information to the COS in the specific instance. However, FOIPPA authority is permissive, meaning that although these authorities exist for a public body to disclose the information, they are not required to do so in response to your request.

#### 5.2 Recording and Documenting

1. An officer who collects or views personal information, whether or not a record is made of the personal information itself, shall record in reasonable detail the reason for collecting/viewing it, including without limitation:
  - a. the time and date that access was made;
  - b. the name of the individual whose personal information was collected;
  - c. the reason (as authorized under FOIPPA) for collecting the personal information; and
  - d. the associated file number(s) (e.g. COORS number, Human/Wildlife Conflict Report file number, or a file number from an external agency where we are in an assistance role).
2. Files containing personal information and query details will be secured in either electronic or paper format to ensure access to those files is limited to those staff having a legitimate operational need.
3. An officer will maintain a record for at least two (2) years following the collection of the personal information, in a form which will readily permit the tracing of the original request for information to the purpose for the collection of the information.

Note: See COS Business Rules for the Notebook, appended to COS Policy 1.5.01, Operational Administrative Procedures.

### 5.3 Security

1. Officers must ensure members of the public or non-authorized personnel are not provided an opportunity, inadvertently or otherwise, to access, view or overhear confidential or protected information that is beyond that permitted for their level of security screening.
2. The unauthorized access, use, disclosure or disposal of personal information must be reported to the Office of the Government Chief Information Officer ("OCIO").
  - a. An officer will immediately report such an incident to their supervisor.
  - b. The supervisor will immediately report the incident to
    - i. the Shared Services BC Service Desk (available 24 /7) at 250-387-7000 or 1-866 660-0811 and selecting option 3; state that you are reporting a 'security incident' and provide your name and contact information only; and
    - ii. the Ministry Chief Information Officer.
  - c. In the event a supervisor is unavailable, the officer will report the incident.
3. For complete details on responding to unauthorized access, use, disclosure or disposal of personal information ("privacy breach"), see the following documents and tools from the Office of the Chief Information Officer:
  - a. Process for Responding to Privacy Breaches: The document sets out the steps that ministries must follow when responding to a privacy breach. It must be read in conjunction with the Information Incident Management Process.
  - b. Information Incident Checklist: The checklist provides high-level guidance for responding to information incidents.
  - c. Easy Guide for Information Incidents: The document outlines four easy steps to guide workers who encounter information incidents, including a privacy breach.
  - d. Information Incident Report Form: While this form has been developed to support the information incident process, you will not need to complete it in every instance. The OCIO will notify you if you need to complete the form.

New text, added December 16, 2014.