EC50 SECURITY & PRIVACY MANAGEMENT OF RECORDS, INFORMATION & DATA EC50

Effective Date: 01 March 2009
Last Reviewed/Revised Date: 19 June 2025*

Contents

POLICY

1. The Chief Constable shall seek to ensure the security and confidentiality of Delta Police Department (Department) records, information and data, as required by law, and to protect investigative, operational and administrative processes.

2. Department employees must not access, use or disclose any Department record, information or data except as required by the duties of their position, or authorized by Procedures pursuant to this Policy.

3. All records, information and data created by employees in relation to the duties of their position, or coming into their possession as a result of Department operations are, and remain, the property of the Department.

4. Disclosure of records, information or data, whether or not they contain personal information, may only take place in accordance with the B.C. *Freedom of Information and Protection of Privacy Act* (FIPPA), other applicable law, and Department policy.

5. The Chief Constable is designated as 'head' of the Department for the purposes of the *FIPPA*, and may delegate associated responsibilities, as permitted by the *FIPPA.*

6. Investigative records shall be maintained entirely or in relevant part in the Police Records Information Management Environment (PRIME), Digital Evidence Management System (DEMS) or a Major Case Management (MCM) file.

7. The disclosure of records, information or data not specifically covered in this Policy shall be referred to legal counsel or the Coordinator, Information & Privacy Unit (Information & Privacy Coordinator) for direction.

REASON FOR POLICY

8. To seek to ensure only authorized access to, use of, and disclosure of Department records, information and data.

RELATED POLICIES

CS41 – Media Liaison and Release of Information
DP30 – Authorized Access & Use of Electronic Systems
DP31 – Operational Communications Equipment & Use
EC11 – Conflict of Interest
EC51 – Correspondence
EM10 – Employee Files
IP32 – Private & Invisible Records
IR44 – Duty to Warn

PROCEDURES

General

9. Records to be provided to the RCMP or other Canadian security agencies are to be stamped or marked as follows, and stamped or marked records received are to be protected accordingly, to allow for their proper management and protection:

   a) **Protected C – Extremely Sensitive**: information that, if compromised, could reasonably be expected to cause extremely grave injury, at less than the national interest level;

   b) **Protected B – Particularly Sensitive**: information that could cause severe injury or damage to the people or group involved if it was released; and

   c) **Protected A – Low Sensitivity**: information that should not be disclosed to the public without authorization and could reasonably be expected to cause injury or harm.

10. Any employee storing or transporting Department records, information or data, which contain personal, investigative or otherwise sensitive operational information, may only do so on Department secure password protected networks, systems or devices, as provided by the Information Technology Section, and similar paper records must be stored and transported so as to ensure their physical security.

Information Requests – Law Enforcement Agencies

11. Records, information or data may be released to other law enforcement agencies, if requested in writing, in support of an ongoing investigation or for other law enforcement purposes.

12. Requests from law enforcement agencies for records, information or data shall only be considered where the identity and position of the requester is verified.

13. Employees may not release records, information or data where there is potential to compromise an investigation, prosecution or trial, or to jeopardize the health or safety of any person.

14. When investigative records, information or data are disclosed to an outside agency, it shall be documented in the general occurrence report.

15. Under no circumstances will original records be released to any person or agency, except as required by law.

16. If necessary to attempt to restrict any further release, each page of a record copied and released to an outside agency must be printed with the following:

> **CONFIDENTIAL**
> This record is supplied for your information only. It is not to be made known to any other agency or person without the written permission of the DELTA POLICE DEPARTMENT.

17. Any employee receiving a request to provide administrative assistance to another police or government agency (e.g., providing reports, manuals, or other materials, whether created by the Department or commissioned from consultants), must complete a Materials Sharing Agreement (Form 87) and provide the same to the Chief Constable and the Chief Constable of the requesting agency for signature, and if approved, submit a copy of the signed agreement to the Office of the Chief Constable for filing.

Release of Records

General

18. Employees may not access, copy, disclose or otherwise use Department records, information or data for a personal purpose, except with the permission of the Deputy Chief Constable.

19. Requests from non-police agencies for records containing investigative or personal information are to be forwarded to the Information & Privacy Coordinator, who shall review requests received and process and respond to them in accordance with the requirements of the *FIPPA*.

20. Verbal requests from non-police agencies for records may be considered where exigent circumstances exist that prevent a written request, and shall be referred to the Information & Privacy Coordinator or Department legal counsel, or where neither are available, to the Duty Officer or delegate, to consider responding in accordance with the disclosure provisions of the *FIPPA*.

Persons Involved in a Motor Vehicle Collision

21. A person involved in a motor vehicle collision may be provided with the relevant driver copy of a MV6020.

Crown Counsel

22. Court Services staff and members may provide investigative records, information or data to Crown counsel as required for the prosecution of a matter.

Insurance Companies, Lawyers & Other Agents

23. If an insurance company, lawyer or other agent requests a record on the behalf of their client, the request shall be forwarded to the Information & Privacy Coordinator.

Private Individuals

24. All requests by individuals for Department records, whether or not they are named in the records, shall be forwarded to the Information & Privacy Coordinator.

City of Delta

25. The following requests for records from the City of Delta, including from Delta's municipal solicitor, are to be forwarded to the Information & Privacy Coordinator for processing:

    a) requests for records for the purposes of a lawsuit where the City, the Department, the Police Board or any Police Board employee has been named as a party;

    b) requests that are not in relation to a lawsuit involving the Department, the Police Board or Police Board employee; and

    c) requests for records in relation to a claim or lawsuit not involving the Department, and in which the Department involvement is limited to only having investigated the incident.

Researchers

26. Any research requests shall be forwarded to the Information & Privacy Coordinator for assessment and *FIPPA* compliance, and is subject to approval by the Chief Constable.

27. All requests for statistical information not filed through the Information & Privacy Coordinator shall be forwarded to the Corporate Services Manager, to determine the appropriate section of the Department that will be responsible for compiling and releasing the statistics.

Public or Limited Warning Disclosures

Note:
The disclosure of information from law enforcement records, about a person, must balance the person's right to privacy against any intended protection of others. If considering such a disclosure to warn others of a risk posed, consultation with legal counsel ought to take place.

28. The public disclosure of personal information to affect a public or more limited warning from Departmental records is made under the authority of the Chief Constable or delegate, and under no circumstances are Department employees to issue such a warning without prior approval through the chain of command.

29. The Chief Constable:

    a) may authorize the disclosure of information about a person, if it is established that compelling reasons exist which may impact the health or safety of another individual or group of individual; and

    b) must authorize the disclosure of information about a person, if the person poses a risk of significant harm to the health or safety of the public or a group of people, or the disclosure is otherwise clearly in the public interest.

30. Any employee who comes into possession of information that falls within the criteria set out directly above, must immediately bring that information to the attention of the Information & Privacy Coordinator or the Chief Constable, in writing.

31. If information about a person is disclosed to warn others, notice of the disclosure must be mailed to the last known address of the individual, at

the same time or before the disclosure is made; however, notice is not required to be mailed or otherwise provided, if providing the notice could harm the health or safety of an individual or group of individuals.

32. A request to the Chief Constable for approval to warn must describe:

a) the risk to the environment, public or individuals;

b) the urgency of the matter;

c) how the disclosure of the personal information will protect those at risk; and

d) where disclosure is required, the recommended method and target for release.

33. In determining the level of risk, the Chief Constable must consider, as available:

a) the history of the individual including criminal history;

b) the information provided about the individual by any correctional facility or program;

c) any medical services the individual may have received and the individual's response to the same;

d) the individual's access to potential victims;

e) the imminence of the risk and potential the degree of harm anticipated;

f) any interim measures that may be taken to remove the risk of harm other than disclosure;

g) the public's need to know the risks to which they are exposed, and to make informed decision about those risks;

h) less intrusive means that may be used to manage the risk of harm;

i) whether the disclosure is likely to lessen the risk of harm; and

j) whether the disclosure could reasonably be expected to result in physical harm to any individual.

Privacy Management Program

34. The Information & Privacy Coordinator and Department legal counsel are responsible for:

    a) privacy-related matters and providing related direction;

    b) supporting the development, implementation, and maintenance of privacy policies and procedures; and

    c) supporting the Department's compliance with the *FIPPA*.

Information Sharing Agreements & Services Contracts

35. Employees seeking to pursue, or having been approached by another agency or business to enter into an agreement or services contract that includes either the one time or repeated sharing of records, data or information, whether or not that includes information about identifiable individuals, must:

    a) consult with the Information & Privacy Coordinator;

    b) ensure that any agreement is in writing;

    c) if the agreement or contract makes the other agency or business a service provider to the Department, ensure that the agreement or contract specifies that agency or business automatically also becomes subject to the *FIPPA* with respect to any information, data or records obtained from the Department;

    d) have the Information & Privacy Coordinator sign off that the agreement ensures the *FIPPA* requirements for the collection, retention, use and any further disclosure of personal information are met; and

    e) obtain the approval and signature on the agreement by the Chief Constable.

'Privacy Impact Assessment' Requirements

36. Employees seeking to pursue an initiative (whether a project, program, activity or system) involving the collection, use or disclosure of personal identifier information, must:

a) consult with the Information & Privacy Coordinator to determine whether the initiative is of a type for which the *FIPPA* requires that a Privacy Impact Assessment (PIA) be undertaken;

b) if a PIA is required, work with the Information & Privacy Coordinator to complete a written PIA in accordance with requirements of the *FIPPA*; and

c) sign the PIA, and have it signed by the Information & Privacy Coordinator and the Chief Constable, before implementing the initiative.

37. The Information & Privacy Coordinator must retain a copy of every completed and signed PIA.

Privacy Complaints & Breaches

38. An employee who becomes aware, or to whom it is reported, as a complaint or otherwise, that Department held information, data or records has been lost, stolen or disclosed contrary to this or other Department policies (hereafter referred to as a 'privacy breach'), must, as soon as practicable, report the alleged breach to the Chief Constable and the Information & Privacy Coordinator.

39. When being notified of a privacy breach, the Chief Constable must:

a) take all reasonable steps to seek to stop the breach and secure compromised information;

b) have the matter investigated;

c) if personal identifier information was compromised, determine whether to notify affected individuals and the B.C. Information & Privacy Commissioner, based on whether the breach could reasonably be expected to result in significant harm to the individual, including identity theft or other applicable factors contained in the *FIPPA*; and

d) seek recommendations for preventing a similar breach from reoccurring and direct which recommendations are to be implemented.

Records of Incidents Involving Employees

40. When an employee of the Delta Police Board is involved in an on-duty incident (such as being the victim of an offence) or is otherwise acting for the Department while off-duty, the following identifying information shall be collected and entered on PRIME:

    a) agency issued identifying number (e.g., badge number, regimental number, payroll number) to be entered in lieu of last name;

    b) date of birth;

    c) gender;

    d) employer;

    e) occupation; and

    f) business address.

41. When an employee is involved in any off-duty incident (the employee is not acting as an agent of the Department), the employee's information shall be handled as for any other citizen; however, if a member, while off-duty, sees an incident occurring and becomes involved in an official capacity as a police officer, the member is then considered on-duty and the requirements of this Policy shall apply.

42. Where an employee is involved in an incident (on-duty or off-duty) which becomes the subject of a police investigation, a statutory investigation, internal investigation, or public complaint:

    a) all relevant information shall be entered on PRIME; and

    b) to protect the integrity of the investigation, such file is to be made private or invisible as appropriate, in accordance with Policy IP32 – *Private and Invisible Records*.

Employee Specific Personal Information

43. Requests from individuals no longer employed by the Department, for copies of records they created during their employment, will be processed by the Information & Privacy Coordinator in accordance with the *FIPPA.*

44. No employee shall query themselves on PRIME, or any other investigative database, or have any other employee access such a system on their behalf, and any such attempt will be considered a violation of policy and a misuse of police information systems.

45. Any employee seeking personal access to records concerning themselves shall apply to obtain a copy of any existing records by way of a formal *FIPPA* request.

46. Any employee who suspects that a database contains incorrect information about them may apply in writing to the Inspector i/c Human Resources requesting a check, where the employee shall specify reasons for their belief that information is incorrect.

47. If the Inspector i/c Human Resources identifies that a record belonging to the Department contains incorrect information about an employee, the error shall be rectified.

48. If the Inspector i/c Human Resources identifies a record belonging to another agency containing incorrect information about an employee of the Department, the Inspector shall request, including reasons, that the agency rectify the error.

*Revised Dates:
07 February 2013
01 April 2015
28 April 2016