AE16 SECURITY AND CONFIDENTIALITY OF RECORDS AND INFORMATION AE16

Effective Date: 01 March 2009
Revised Date: 12 April 2016
Last Reviewed Date: 28 April 2016

POLICY

1. The Delta Police Department ("Department") will establish and maintain a records management function that will:

   a) ensure the security and confidentiality of designated confidential information and Department records and documents;

   b) ensure that disclosure of information from Department records is consistent with case law and the applicable provincial and federal legislation; and

   c) ensure compliance with the privacy provisions of the *Freedom of Information and Protection of Privacy Act* ("FOIPPA").

REASON FOR POLICY

2. To provide for the access to, and confidentiality of, the Department records.

RELATED POLICY

AC30 – Communication Rules
AE12 – Private and Invisible Records
OC20 – Media Liaison and Release of Information
OC31 – Duty to Warn

PROCEDURES

Operational Records, Security and Access

3. All records created and coming into the possession of the Department through the operation of the Department are, and remain, the property of

the Department. Control of and access to records must occur only in accordance with the FOIPPA and with established policy and procedure.

4. A member of the Department must not:

   a) access, or attempt to access, any record which they are not specifically authorized to use;

   b) use Department records for an unauthorized purpose; or

   c) use police computer systems or records for personal gain or benefit to themselves or to another person.

5. Law enforcement and other government agencies may designate information at specific "Protected" levels. As with all other records, access, use and disclosure of protected information requires proper authorization. The following sets out the type of information at each protected level:

   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.

   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.

6. Any member who obtains unauthorized access to a record will be personally liable for any use or disclosure of the record resulting from the unauthorized access.

Release of Information by Members

7. Any Delta member may release:

   a) a copy of the driver copy of a MV6020 to any person involved in a motor vehicle accident;

b) copies of records to Crown counsel for the prosecution of a matter; and

c) information, or a copy of a record, to a law enforcement agency for a law enforcement purpose.

Record Security - Information Services

8. Access to Information Services Branch hardcopy master files storage areas is restricted to Branch staff whose immediate duties require that they have access to hardcopy files.

9. Information Services Branch staff will be available seven (7) days a week, twenty-four (24) hours a day to retrieve files.

10. Hardcopy master files may be removed from Information Services Branch file storage areas by the Information Services Branch staff only, and records are to be re-shelved only by the Information Services Branch staff.

11. All hardcopy master files must be maintained as follows:

a) a master file must not be taken from its designated storage area, except for access by Branch staff or if approved by the Information Services Manager, and in either case must be signed out on the File Tracker;

b) where no operational or legal requirement for taking the original master file exists, a photocopy of the contents of the master file will be provided;

c) the person signing out a file will be responsible for it and must ensure that the file is returned to its designated storage area as soon as possible; and

d) any person requesting to view a hardcopy master file will have the file signed out on File Tracker for the duration of their viewing to record when the file has been accessed.

Record Security – CIB

12. Files in the Major Case Management ("MCM") system will be maintained in line with CIB operating procedures. All requirements for release and protection of information contained in this policy and related policies apply to files in the MCM system.

Release of Records to non-Police Agencies

13. Requests from non-police agencies for records must be in writing and on the letterhead of the agency requesting access to the records.

14. All written requests for information must be forwarded to the Information and Privacy Coordinator, except requests for those records that either a member or the Information Services Branch Manager has authorization to release under this policy and procedure.

15. If a request is to be answered by correspondence, that request must be forwarded to the Information and Privacy Coordinator for authorization.

16. Verbal requests from non-police agencies for records may be considered where exigent circumstances exist that prevent a written request and must be referred to the Information and Privacy Coordinator or, where the Coordinator is not available, the Staff Sergeant, to be responded to in accordance with the disclosure provisions of the FOIPPA.

Release of Records to Law Enforcement Agencies

17. Requests from law enforcement agencies for records may be considered where the information is required for an on-going investigation or for another law enforcement purpose.

18. Telephone requests from law enforcement agencies for access to a record will be considered only where the identity and position of the requester is verified by a telephone call to the requester's agency or a facsimile or e-mail message is received for verification.

19. No record, or other information, will be disclosed in the initial telephone contact or prior to the requester's identity being verified.

20. Access to a record may be denied where there is a possibility that access might:

    a) compromise an investigation, prosecution or trial;

    b) reveal investigative techniques or operations; or

    c) jeopardize the health or safety of any person.

21. Each time access to a general occurrence file is granted to an outside agency, the person providing access must document access in the general occurrence report.

22. Under no circumstances will original records be released to any person or agency.

23. Each page of a record copied and intended for release to an outside agency must be stamped with the following:

> **CONFIDENTIAL**
> This police report is supplied to you 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.

24. Requests for access to records not covered in this policy and procedure must be forwarded to the Information and Privacy Coordinator.

Public Disclosures in Accordance with Sections 25 and 33 of the FOIPPA

25. The public disclosure of information about an individual from law enforcement records requires a delicate balance between the individuals' right to privacy versus disclosure to protect others. In appropriate cases, the Department may consult with legal counsel to determine if the concern for public safety outweighs the potential civil liability of the privacy invasion.

Assessing For Section 33 Release

26. Under Section 33 of the FOIPPA, a public body may disclose personal information if the head of the public body determines that compelling

reasons exist that may impact the health or safety of an individual or group of individuals.

27. If personal information is disclosed, notice of disclosure must be mailed to the last known address of the individual informing them the information is about to be disclosed and mailed at the same time or before the disclosure is made. 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.

28. While Section 33 of the FOIPPA grants the discretion to release personal information, Section 25 of the FOIPPA imposes a duty on the Chief Constable to disclose to the public, or an identifiable affected group, information:

    a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or

    b) the disclosure of which is clearly in the public interest.

29. This duty will exist whether or not a request for access is made, and may require the release of personal information that would otherwise be protected by the privacy provisions of the FOIPPA.

30. Any member of the Department who comes into possession of information that falls within the criteria set out in Section 26 must immediately bring that information to the attention of the Information and Privacy Coordinator or the Chief Constable, in writing.

31. The public disclosure of personal information from Departmental records is made under the authority of the Chief Constable or delegate. Under no circumstances are Department employees to disclose such information without prior approval through the chain of command.

    (See also: Policy **OC20 — Media Liaison and Release of Information**)

Assessing Information for a FOIPPA Section 25 or 33 Release

32. A request for approval to release personal information under Section 25 or 33 of the FOIPPA 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 appropriate method and target for release.

33. In determining the level of risk to the environment, public or individual, consideration must be given to all the relevant circumstances and, where the risk is posed by an individual, that consideration may include:

a) the history of the individual including criminal history and criminal convictions;

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

c) any treatment the individual may have received and the individual's response to the treatment;

d) any relevant psychiatric information;

e) the individual's access to potential victims;

f) the individual's current residential and employment status where relevant;

g) relevant expert advice where immediately available and accessible; and

h) any other relevant information about the individual.

34. In determining the urgency of the matter, consideration must be given to all the relevant circumstances, including:

a) the imminence of the risk;

b) the level of harm anticipated;

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

d) the right of the public to know the risks to which they are exposed and the right to make informed decision about those risks.

35. In determining whether to recommend disclosure of information under Section 25 of the FOIPPA, consideration must be given to all the relevant circumstances including whether:

a) less intrusive means may be used to remove the risk of harm;

b) the disclosure is likely to lessen the risk of harm; or

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

36. Where it is assessed that personal information must be released under Section 25 of the FOIPPA, and having regard to the extent of the disclosure required, the means by which the disclosure should occur will be determined by the Chief Constable, or designate.

Criminal Records

37. Any Department member may release the criminal record of an accused person to Crown counsel for the purpose of prosecuting a matter, but Crown counsel requests for the criminal record of any other person must be forwarded to the Court Services Supervisor.

38. All requests by individuals for their criminal record are processed through the Information and Privacy Unit.

39. In the case of personal written requests for criminal records checks, possible "hits" may be verified by way of fingerprint submission to RCMP, Ottawa.

Insurance Companies, Lawyers and Other Agents

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

41. A request from an insurance company, lawyer, or other agent for information other than the MV6020 must be forwarded to the Information and Privacy Coordinator.

Requests from the City of Delta

42. The City of Delta or the Municipal Solicitor may request and receive copies of 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 to the suit.

43. Requests from the City of Delta or the Municipal Solicitor that are not in relation to a lawsuit involving the Department, the Police Board or Police Board employee, must be referred to the Information and Privacy Coordinator.

44. Requests from the City of Delta or the Municipal Solicitor 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, are subject to the disclosure provisions in the FOIPPA and must be referred to the Information and Privacy Coordinator for processing.

Research Requests

45. The FOIPPA allows for access by third parties to the Department records for research purposes, however, such access is at the discretion of the Department and must be in accordance with strict limitations and procedural requirements set out in the FOIPPA. Any research request must be forwarded to the Information and Privacy Coordinator for assessment and is subject to approval by the Chief Constable.

Records of Incidents Involving Employees

46. 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 will 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.

47. 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 will 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 Section 46 above will apply.

48. 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, all relevant information will be entered on PRIME. To protect the integrity of the investigation, such file will be made private or invisible as appropriate, in accordance with **Policy AE12 Private and Invisible Records**.

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

50. Any employee seeking personal access to records concerning themselves, must apply to obtain a copy of any existing records by way of a formal FOIPPA request.

51. Any employee who suspects that a database contains incorrect information about him or her may apply in writing to the Inspector or Staff Sergeant of Human Resources and Administration, requesting a check. The employee must specify reasons for their belief that information is incorrect and may not request a check without specific and reasonable cause.

52. If the Inspector or Staff Sergeant identifies that a record belonging to the Department contains incorrect information about an employee, the error shall be rectified.

53. If the Inspector or Staff Sergeant identifies a record belonging to another agency contains incorrect information about an employee of the Department, the Inspector or Staff Sergeant shall request, in writing, including reasons, that the agency rectify the error.

Freedom of Information and Protection of Privacy Act

54. All requests received by the Department under the FOIPPA must be processed in accordance with the policy and procedure set out in this policy.

55. The records held by the Department are of a confidential nature and the Department has, as one of its responsibilities, the duty to protect its records from any unauthorized disclosure or access. It will be the duty of each member and employee of the Department to ensure that no unauthorized disclosure of or access to records occurs.

56. This section of the policy does not apply to requests for access to records containing personal information covered by other Information Services Branch records disclosure policies, however, such policies must also be in compliance with the provisions of the FOIPPA.

57. The Chief Constable of the Department is designated as "head" of the Department for the purposes of the FOIPPA. The Information and Privacy Coordinator will be responsible for the Administration of the FOIPPA within the Department. The Coordinator will report to the Information Services Manager.

58. A person receiving a request under the FOIPPA must forward it to the Coordinator within one day from the day the request is received.

59. The Coordinator must review the request to ensure it complies with the requirements of a formal request under the FOIPPA. The request will then be logged in the Information and Privacy File Tracking System and an FOI file opened. The Information and Privacy Coordinator retains the original request, and may contact the applicant to clarify and refine a request.

60. A request may be transferred to another public body, under s. 11 of the FOIPPA, after consultation with the other public body and if the record requested:

    a) was produced by or for another public body;

    b) was first obtained by another public body; or

    c) is in the custody or control of another public body.

61. The Coordinator must determine the extent of the search necessary to locate requested records and estimate the search time required. Where authorized by the FOIPPA, the Coordinator must prepare an estimate of the fee for processing a request, but may consider waiving any fee less than $100.00 pursuant to Section 75(5) of the FOIPPA. Fees in excess of $100.00 may be waived only by the Deputy Chief Constable of Administration.

62. If it is determined that a deposit is required before processing can proceed:

    a) processing of a request must stop once a letter of acknowledgement and fee estimate have been sent to the applicant; and

    b) processing of the request must not continue until the deposit is paid in full by the applicant.

63. As soon as is practicable, but no later than 7 working days from the date a request is received:

    a) the Coordinator must send the applicant a letter acknowledging receipt of request or make contact by telephone; and

    b) the letter or phone call must specify the name of a person to whom the applicant may direct questions about the processing of the request.

64. Section 63 does not apply where a request has been processed within 7 working days of having been received and a complete response has been sent to the applicant within that time.

Search and Retrieval of Records Requested

65. In this policy, the term "records" will include: original files, working files, notes, members notebooks, marginal notes, drawings, maps, photographs, videotapes, and information stored by any electronic means.

66. The Coordinator must send a written request or email to each Branch of the Department that may, in the opinion of the Coordinator, have control or custody of records subject to a request.

67. Where the person in charge of a Branch receives a request for records from the Coordinator, the person in charge will be responsible for a thorough search of the records held within the Branch and must provide the records requested or exact copies thereof, to the Coordinator as soon as practicable after receiving a request.

68. Upon the completion of a search for records, whether or not any of the records requested are located, the person in charge of the Branch must send the records to the Coordinator, along with the following information:

    a) a description of the search conducted in the Branch;

    b) a description of where the records were located;

    c) if requested by the Coordinator, an exact report of the time spent searching for and retrieving the records including the name of the person who conducted the search and the date (excluding photocopying time);

    d) notice of any relevant records that have been destroyed or transferred to another site and, where a record has been transferred, the current location of that record;

    e) notice if a requested record will have to be created from a computer or other electronic record; and

    f) notice of any reason the record should be protected or whether the record, or any portion of it, was received in confidence.

69. Where, due to the number of records requested, it is expected that there will be a delay in producing them, the person in charge of a Branch must notify the Coordinator immediately.

Third Party Notice

70. Where a request is received for a record that contains the personal information of an individual, other than the applicant, Section 22 of the FOIPPA must be considered.

71. Where the Coordinator intends to grant access to a record that contains the personal information of a third party, the Coordinator must ensure the

third party is provided notice, in the prescribed form, as is required under Section 23 of the FOIPPA.

Consultation with Investigator

72. Prior to making an access or non-disclosure decision, the Coordinator may consult with the member responsible for the investigation of a general occurrence file.

73. In consulting with the investigator, the Coordinator must determine if the disclosure of a record involves any potentially sensitive issues or whether any record was provided to the Department in confidence.

Record Analysis and Response Preparation

74. The Coordinator must analyze each record requested, line by line, and carefully consider the applicability of all exceptions provided under the FOIPPA.

75. Where appropriate, the Coordinator may except records and sever excepted portions of records in accordance with the FOIPPA.

76. It will be the duty of the Coordinator to apply the statutory exceptions in a judicial manner, being careful to balance the right to access with the protection of law enforcement matters and the protection of the personal privacy of others.

77. The Coordinator must prepare a response for each request. The response must:

    a) comprise a letter and copies of any records available to the applicant after an analysis has been completed; and

    b) comply with Section 8 of the FOIPPA; and

    c) inform the applicant:

        i) whether or not the applicant will be granted access;

        ii) if the access is to be granted, where, when and how access will be given;

iii) if access to a record or portion thereof is denied, the reasons for the denial and the statutory authority for the denial;

iv) the name of a contact person to whom the applicant may direct any questions;

v) if access is denied, that there is a right of appeal to the Information and Privacy Commissioner, and

vi) where appropriate, the full address of the Information and Privacy Commissioner.

Authority to Release a Response

78. Unless it is necessary to have the applicant attend the Department to provide proof of identification, the Coordinator may send a response by regular mail, registered mail or courier.

79. The FOI Coordinator is responsible for complying with formal requests for information access under the FOIPPA. The Coordinator has delegated authority under the FOIPPA. The Coordinator will sign the information released under the FOIPPA.

80. The Coordinator will represent the Department in any dealings with the Office of the Information and Privacy Commissioner ("OIPC") unless the complexity of the issues warrant legal representation.

81. For the purposes of FOIPPA, documentation generated in response to a request for access under the FOIPPA must be retained for a period of at least one year pursuant to Section 31 of the FOIPPA.