| | | | |
|---|---|---|---|
| **Policy Name:** | **SECURITY AND CONFIDENTIALITY OF RECORDS AND INFORMATION** | | |
| **Policy #:** | AD 9.18 | **Last Updated:** | 2021-12-03 |
| **Issued By:** | SUPPORT SERVICES BUREAU | **Approved By:** | SURREY POLICE BOARD |
| | | **Review Frequency:** | AS REQUIRED |

**RELATED POLICIES**

AD 9.1 Authorized Use of Computing Environment and Electronic Communications

AD 9.15 Security Clearance

AD 9.19 Information Technology (IT) Security

## 1. PURPOSE

1.1. To provide for the access to, and confidentiality of, Surrey Police Service (SPS) records.

1.2. To provide requirements under the *Freedom of Information and Protection of Privacy Act* (FOIPPA) relating to the public disclosure of personal information.

1.3. To ensure all Employees operate communication equipment, communication devices, and software in accordance with statutory law and SPS policy

## 2. SCOPE

2.1. This policy applies to all SPS Employees, Volunteers, Practicum Students and Contractors.

## 3. POLICY

3.1 The SPS will establish and maintain a records management function that will:

i. ensure the security and confidentiality of designated confidential information and SPS records;

ii. ensure that disclosure of information from SPS records is consistent with case law and the applicable federal and provincial legislation; and

iii. ensure compliance with the privacy provisions of FOIPPA, including preserving the anonymity of applicants under FOIPPA, except where necessary to process requests for records under FOIPPA.

## 4. PROCEDURE

**Operational Records, Security and Access**

4.1. All records created and coming into the possession of the SPS through the operation of the SPS are, and remain, the property of the SPS. Control of and access to records must occur only in accordance with FOIPPA and with SPS records management policies and procedures.

4.2. An Employee, Volunteer, Practicum Student, or Contractor must not:

i. access, or attempt to access, any record which they are not specifically authorized to use;
ii. use SPS records for an unauthorized purpose; or
iii. use police computing environment, electronic communications or records for personal gain or benefit to themselves or to another person.

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

i. 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.
ii. Protected B – Particularly Sensitive: information that could cause severe injury or damage to the people or group involved if it was disclosed.
iii. Protected C – Extremely Sensitive: information that, if compromised, could reasonably be expected to cause extremely grave injury, at less than the national interest level.

4.4. An Employee, Volunteer, Practicum Student, or Contractor who obtains unauthorized access to a record may be personally liable for any use or disclosure of the record resulting from the unauthorized access.

**Disclosure of Information by Members**

4.5. Any Member or civilian employee may disclose:

i. a copy of the driver's copy of a MV6020 to any person involved in a motor vehicle collision;
ii. copies of records to Crown Counsel for the prosecution of a matter; and
iii. information, or a copy of a record, to a law enforcement agency in Canada for a law enforcement purpose.

**Records Security - Information Management Services**

4.6. Access to Information Management Services (IMS) master files storage areas is restricted to employees whose duties require that they have access to these files.

4.7. IMS Employees will be available seven (7) days a week, twenty-four (24) hours a day to retrieve files.

4.8. Hardcopy master files may be removed from IMS file storage areas by the IMS staff only, and records are to be re-shelved only by IMS staff.

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

i. a master file must not be taken from its designated storage area, except for access by IMS Employees or if approved by the Manger, IMS, and in either case must be signed out by the Employee or Member;
ii. 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;
iii. 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
iv. any person requesting to view a hardcopy master file will have the file signed out for the duration of their viewing to record when the file has been accessed.

**Records Security – Investigative Services Bureau**

4.10. Files in the Major Case Management (MCM) system will be maintained in line with Investigative Services Bureau (ISB) operating procedures. All requirements for disclosure and protection of information contained in this policy and related policies apply to files in the MCM system.

**Disclosure of Records to non-Police Agencies**

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

4.12. All written requests for information must be forwarded to the Manager, Information and Privacy Unit (IPU), except requests for those records that either a Member or the Manager, IMS has authorization to disclose under this policy and procedure.

4.13. If a request for records is to be answered by correspondence, that request must be forwarded to the Manager, IPU for authorization.

4.14. 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 Manager, IPU or, where the Manager, IPU is not available, the Manager, IMS to be responded to in accordance with the disclosure provisions of FOIPPA.

**Disclosure of Records to Law Enforcement Agencies**

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

4.16. 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.

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

4.18. Access to a record may be denied where access could reasonably be expected to:

i. compromise an investigation, prosecution or trial;
ii. reveal investigative techniques or operations; or
iii. jeopardize the health or safety of any person.

4.19. Each time access to a General Occurrence (GO) report is granted to an outside agency, the person providing access must document access in the GO report and tracked via “Release Tracking” feature in PRIME.

4.20. Under no circumstances will original records be disclosed to any person from an outside agency.

4.21. Each page of a record copied and intended for disclosure 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 advance written permission of the Surrey Police Service.”*

4.22. Requests for access to records not covered in this policy and procedure must be forwarded to the Manager, IPU.

**Public Disclosures and the Duty to Warn**

4.23. The public disclosure of information about an individual from law enforcement records requires a balance between the individual's right to privacy versus disclosure to protect others. SPS may consult the General Counsel, SPS Legal Services to determine if the duty to warn the public outweighs the potential invasion of personal privacy and potential civil liability for the disclosure.

4.24. In accordance with s. 33.1(m) FOIPPA, SPS may disclose personal information if the SPS Chief Constable determines that compelling reasons exist that may affect the health or safety of an individual or group of individuals.

4.25. If personal information is disclosed under s. 33.1(m) FOIPPA, notice of disclosure will be mailed to the last known address of the individual notifying them the information is about to be disclosed. This notice must be 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.

4.26. Section 25 FOIPPA imposes a duty on the Chief Constable or delegate to disclose to the public, or an affected group of people, or to an applicant, information:

i. about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or
ii. the disclosure of which is, for any other reason, clearly in the public interest.

4.27. This duty exists whether a request for access is made and may require the disclosure of personal information that would otherwise be protected by the privacy provisions of FOIPPA.

4.28. Public disclosure of personal information from SPS records is made in accordance with FOIPPA and under the authority of the Chief Constable or delegate. Under no circumstances are SPS Employees to disclose personal information or records to the public or media without prior approval through the chain of command.

4.29. A request for approval to disclose personal information must describe:

i. the risk to the environment, public or individuals;
ii. the urgency of the matter;
iii. how disclosure of the personal information will protect those at risk; and
iv. where disclosure is required, the appropriate method and target for disclosure.

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

i. the history of the person including criminal history and criminal convictions;
ii. the information provided about the individual by any correctional facility or program;
iii. any treatment the individual may have received and the individual's response to the treatment;
iv. any relevant psychiatric information;
v. the individual's access to potential victims;
vi. the individual's current residential and employment status where relevant;
vii. relevant expert advice where immediately available and accessible; and
viii. any other relevant, credible and recent information about the individual.

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

i. the imminence of the risk;
ii. the level of harm anticipated;
iii. any interim measures that may be taken to remove the risk of harm other than disclosure; and
iv. the right of the public to timely notification of the risks to which they are exposed and the right to make informed decision about those risks.

**Information Requiring Immediate Public Disclosure – the Duty to Warn**

4.32. A Member who believes that it is in the public interest to publicize information that a person poses a risk of significant harm to the public or a group of people, must forward a copy of the report to their Supervisor and to the Manager, IPU prior to the end of shift for immediate attention.

4.33. The Supervisor must:

i. ensure all Members involved in the investigation complete all reports prior to the end of shift; and
ii. forward the reports with comments and recommendations to the Deputy Chief Constable, Investigative Services to ensure the disclosure of information does not jeopardize or hinder an ongoing investigation or operation.

4.34. The Deputy Chief Constable, Investigative Services Bureau or delegate shall determine:

i. the information that is to be disclosed; and
ii. how the information shall be disclosed (e.g., a general media release or a local bulletin release).

4.35. In cases of extreme urgency, the Supervisor shall consult with the Duty Officer to determine if immediate action is required. The Duty Officer shall consider immediate protection measures and the need for a direct response, which may include, but is not limited to, the disclosure of:

i. sketches;
ii. names and photographs of people involved; and
iii. surveillance photos to assist in identifying suspects.

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

i. less intrusive means may be used to remove the risk of harm;
ii. the disclosure is likely to lessen the risk of harm; or
iii. the disclosure could reasonably be expected to result in physical harm to any individual.

4.37. Where the SPS has decided that personal information must be disclosed under s. 25 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 delegate, in consultation with the General Counsel, SPS Legal Services and the Manager, IPU.

**Criminal Records**

4.38. Any SPS Member may disclose 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.

4.39. All requests by individuals for their criminal record are processed through the Manager, IPU.

4.40. Police Information Checks (with or without Vulnerable Sector checks) are processed as per AD 9.15 *Security Clearance*.

**Insurance Companies, Lawyers and Other Agents**

4.41. If an insurance company, lawyer or other agent requests a record on the behalf of their client, the request must be forwarded to the IPU.

4.42. A request from an insurance company, lawyer, or other agent for information other than the MV6020 must be forwarded to the IPU.

**Requests from the City of Surrey**

4.43. The City of Surrey or the City Solicitor may request and receive copies of records for the purposes of a lawsuit where the City, SPS, the Surrey Police Board or any Police Board Employee has been named as a party to the suit.

4.44. Requests from the City of Surrey or the City Solicitor that are not in relation to a lawsuit involving SPS, the Surrey Police Board or Police Board Employee, must be referred to the Manager, IPU.

4.45. Requests from the City of Surrey or the City Solicitor for records in relation to a claim or lawsuit not involving SPS, and in which SPS involvement is limited to only having investigated the incident, are subject to FOIPPA disclosure provisions and must be referred to the IPU for processing. Court orders, summonses and subpoenas may be required prior to disclosure.

**Research Requests**

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

**Records of Incidents Involving Employees**

4.47. When an Employee of the Surrey Police Board is involved in an on-duty incident (such as being the victim of an offence) or is otherwise acting for the SPS while off-duty, the following identifying information will be collected and entered on PRIME:

i. agency issued identifying number (e.g. badge number, payroll number) to be entered in lieu of last name;
ii. date of birth;
iii. gender;
iv. employer;
v. occupation; and
vi. business address.

4.48. When an Employee is involved in any off-duty incident (the Employee is not acting as an agent of SPS), the Employee's information will be handled as for any other resident of the City of Surrey. 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 s. 4.47 above will apply.

4.49. 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.

4.50. No Employee shall query themselves or any other person on PRIME-BC, CPIC, or any other investigative database, or have any other Employee access such a system on their behalf unless it

is for a bona fide duty-related investigational or operational purpose. Any such attempt is a violation of policy, misuse of police information systems, and subject to a *Police Act* investigation.

4.51. Any Employee seeking personal access to records concerning themselves, must apply to obtain a copy of any existing records by way of a written request to the Inspector, Employee Services Section (ESS).

4.52. Any Employee who suspects that a database contains incorrect information about him or her may apply in writing to the Inspector, ESS 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. Under s. 29 FOIPPA, Employees have the right to request correction of their personal information. The Inspector, ESS will contact the Manager, IPU for assistance.

**Freedom of Information and Protection of Privacy Act**

4.53. All requests received by SPS under FOIPPA must be processed in accordance with this policy.

4.54. The records held by the SPS are confidential and the SPS has, as one of its responsibilities, the duty to protect its records from any unauthorized disclosure or access. It is the duty of each Member and civilian Employee of the SPS to ensure that no unauthorized disclosure of or access to records occurs.

4.55. The Chief Constable is the "head" of the SPS under FOIPPA. The IPU is responsible for the administration of FOIPPA within SPS.

4.56. An Employee who receives a request under FOIPPA must forward it to the IPU within one (1) day from the day the request is received.

4.57. The IPU shall review the request to ensure it complies with the requirements of a formal request under FOIPPA. The IPU retains the original request and may contact the applicant to clarify and refine a request.

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

i. was produced by or for another public body;
ii. was first obtained by another public body; or
iii. is in the custody or control of another public body.

4.59. SPS cannot transfer FOIPPA requests to the Royal Canadian Mounted Police and other government institutions under the federal *Access to Information Act* and the federal *Privacy Act*.

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

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

i. processing of a request must stop once a letter of acknowledgement and fee estimate have been sent to the applicant; and
ii. processing of the request must not continue until the deposit is paid in full by the applicant.

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

i. the IPU must send the applicant a letter or email acknowledging receipt of request or make contact by telephone; and
ii. the letter, email, or phone call must specify the name of a person to whom the applicant may direct questions about the processing of the request.

**Search and Retrieval of Records Requested**

4.63. The IPU must send a written request or email to each section of SPS that may, in the opinion of the Manager, IPU have control or custody of records subject to a request.

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

4.65. Upon the completion of a search for records, whether any of the records requested are located, the person in charge of the section must send the records to the Manager, IPU the following information:

i. a description of the search conducted;
ii. a description of where the records were located;
iii. if requested by the Manager, IPU, 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);
iv. 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;

v. notice if a requested record will have to be created from a computer or other electronic record; and
vi. notice of any reason the record should be protected or whether the record, or any portion of it, was received in confidence.

4.66. 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 the section must notify the Manager, IPU as soon as practicable so that an extension under s. 10(1) FOIPPA can be requested as appropriate.

**Third Party Notice**

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

4.68. Where the Manager. IPU intends to disclose a record that contains the personal information of a third party, where that personal information may be eligible for redaction under s. 22 FOIPPA, the Manager, IPU must ensure the third party is provided notice, in the prescribed form, as required under s. 23 FOIPPA.

**Consultation with Investigator**

4.69. Prior to making an access or non-disclosure decision, the Manager, IPU may consult with the Member responsible for the investigation of a GO file.

4.70. In consulting with the investigator, the Manager, IPU must determine if the disclosure of a record involves any potentially sensitive issues or whether any record was provided to the SPS in confidence.

**Disclosure to Foreign Law Enforcement Agencies**

4.71. When a Member discloses police information about an individual to a foreign law enforcement agency, the Member must create and maintain a detailed GO report. If the disclosure is to further the Member's own investigation, or to assist in an investigation or law enforcement proceeding undertaken by a foreign agency, the Member must create a General Occurrence using the UCR code 8900-6 "assist foreign agency" and record the following details in the report:

i. the agency file number;
ii. the name, position and contact information of the foreign agency Member who requested the disclosure of information and/or to whom information was disclosed;
iii. the purpose for which the information was requested and/or disclosed;
iv. the nature of the information disclosed; and
v. where information is requested and/or disclosed in accordance with a formal written agreement, a treaty or legislative authority, the Member must ensure compliance with the terms of the same.

4.72. Members shall consult the Manager, IPU, if uncertain as to the authorization for disclosure of police information to foreign agencies.

**Record Analysis and Response Preparation**

4.73. The Manager, IPU must analyze each record requested, consider the applicability of all exceptions provided under FOIPPA, and where appropriate, except records and sever excepted portions of records in accordance with FOIPPA.

4.74. The Manager, IPU shall prepare a response for each request. The response must include a letter and copies of any records available to the applicant after an analysis has been completed and 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 Disclose Records to Applicant**

4.75. Unless it is necessary to have the applicant attend SPS to provide proof of identification, the Manager, IPU may send a response by SPS Internet delivery portal, regular mail, registered mail or courier.

4.76. The Manager, IPU is responsible for complying with formal requests for information access under FOIPPA. The Manager, IPU has delegated authority under FOIPPA. The Manager, IPU will sign the information disclosed under FOIPPA.

4.77. The Manager, IPU will represent SPS in any dealings with the Office of the Information and Privacy Commissioner of British Columbia unless the complexity of the issues require legal representation.

4.78. For the purposes of FOIPPA, documentation generated in response to a request for access under FOIPPA must be retained for a period of at least one (1) year pursuant to s. 31 FOIPPA.

**APPENDIX A: DEFINITIONS**

“Computing environment” means any electronic information, information system, application, device (including PCs, laptops, mobile devices, and telephones) or other computing technology that is connected to the SPS’s IT systems (including cloud-based services and mobile services).

“Confidential Information” includes information related to individuals such as Social Insurance Number, banking information, personal information (date of birth, gender, family status), Human Resources records, criminal investigations, criminal records, payroll records, etc. This information is typically not available from alternate sources.

“Contractor” means an individual who has access to SPS Premises, as defined in this Policy, for the purpose of providing services or supplies to the SPS on a contractual basis.

“Coordinator” means the Manager of Information and Privacy Unit.

"CPIC" means the Canadian Police Information Centre, a computerized national repository of information that facilitates the sharing of information among authorized agencies.

“Employee” means any SPS Employee (including Members and civilian staff) appointed by the Surrey Police Board.

“FOIPPA” means the *Freedom of Information and Protection of Privacy Act.*

“IMS” means the Surrey Police Service’s Information Management Services section.

“IPU” means the Surrey Police Service’s Information and Privacy Unit

“Member” means a sworn Police Officer appointed by the Surrey Police Board.

“Practicum Student” means a student of a program at a recognized education institution who is engaged at SPS Premises for study, research, work experience, etc.

“PRIME” means "Police Records Information Management Environment” which connects law enforcement agencies in BC with a single provincial records management system.

"Records" means original files, working files, notes, Members’ notebooks, marginal notes, drawings, maps, photographs, videotapes, and information stored by any electronic means.

“Supervisor” means a Team Leader, Manager, Sergeant, Staff Sergeant, Inspector, Superintendent, Deputy Chief Constable, Chief Constable, and any other person acting in a supervisory capacity who is accountable for a particular area or shift on behalf of SPS.

“Volunteer” means a person serving SPS who is not an Employee, Practicum Student, or Contractor, as defined in this Policy, and includes those individuals serving on any board(s), commission(s) or committee(s) established by SPS.

## APPENDIX B: REFERENCES

*Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c. 165.