Policy Name:	**FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT**		
Policy #:	AD 9.7	**Last Updated:**	2022-06-08
Issued By:	SPS LEGAL SERVICES	**Approved By:**	SURREY POLICE BOARD
		Review Frequency:	AS REQUIRED

RELATED POLICIES

AD 9.18 *Security and Confidentiality of Records and Information*

OP 4.19.1 *Duty to Warn – Public Interest Notification*

1. PURPOSE

1.1. To provide the requirements under the BC *Freedom of Information and Protection of Privacy Ac*t (FOIPPA) which governs Surrey Police Service (SPS) Employees.

1.2. To provide guidance to Employees on the protection and disclosure of Personal Information held in SPS records, in a manner which is lawful and compliant with FOIPPA requirements.

1.3. To provide Employees with direction on reporting and investigating FOIPPA Privacy Breaches.

2. SCOPE

2.1. This policy applies to all SPS Employees.

3. POLICY

3.1. Employees are responsible for protecting Personal Information that is held in SPS's custody and control, maintaining accurate records, and avoiding the disclosure of confidential information of SPS, its members, volunteers or members of the public that is not authorized by FOIPPA.

3.2. Employees have a duty to understand key components of FOIPPA and will follow the provisions set out by FOIPPA.

3.3. SPS will establish guidelines for investigating and reporting privacy breaches that align with FOIPPA requirements.

4. PROCEDURE

4.1. SPS is governed by FOIPPA. Employees must act in accordance with FOIPPA and be aware of their legal responsibilities under FOIPPA.

4.2. Employees should understand the purposes of FOIPPA which is to:

i. give the public the right of access to records;
ii. give individuals a right of access to, and a right to request correction of, Personal Information about themselves;
iii. specify limited exceptions to the right of access;
iv. prevent the unauthorized collection, use or disclosure of Personal Information by public bodies; and
v. provide for an independent review of decisions made under FOIPPA.

4.3. FOIPPA applies to all records in the custody or under the control of SPS. All Employees must:

i. protect the Personal Information in SPS records unless disclosure is provided for in FOIPPA; and
ii. direct individuals requesting access to records held by SPS to the Information and Privacy Unit under SPS policy AD 9.18 *Security and Confidentiality of Records and Information*.

4.4. FOIPPA governs the collection, use, retention, disposal, and disclosure of Personal Information. Employees must ensure Personal Information collected by SPS is:

i. collected in compliance with section 26 (purposes for which Personal Information may be collected) of FOIPPA;
ii. collected using the minimum amount of Personal Information necessary;
iii. used only for the purpose for which it was obtained or otherwise in compliance with FOIPPA;
iv. collected with the consent of the individual to whom the Personal Information pertains;

v. retained for a period of at least one year or longer in compliance with operational and administrative records retention policies; and
vi. disposed of following the approved retention schedule and in a manner following SPS policy for secure records shredding/destruction.

4.5. Employees have a duty under section 28 of FOIPPA to ensure that Personal Information contained in SPS records is accurate and complete.

4.6. Section 29 of FOIPPA gives individuals the right to correct their Personal Information and/or provide additional information if they believe there is an error or omission in their Personal Information in the custody or under the control of SPS. Employees will:

i. make every effort to ensure correct Personal Information is obtained. If an individual requests a correction to their Personal Information that can be verified as correct, and is allowed in accordance with records management policy, the Employee will make every effort to correct Personal Information as requested by the individual; and
ii. if an Employee cannot correct the information, or the information is an opinion, or the information cannot be proven to be correct, the Employee will document or annotate the request without altering the original information in accordance with records management procedures.

4.7. SPS will protect Personal Information in its custody and control by implementing reasonable physical and procedural security measures. Employees will:

i. follow the guidelines for the security of physical and electronic information held by SPS;
ii. understand and follow SPS policy AD 9.18 *Security and Confidentiality of Records and Information*; and
iii. ensure that the disposal and destruction of Personal Information is done according to the requirements of FOIPPA, SPS policy, and records management procedures.

4.8. Disclosure of Personal Information is not authorized under FOIPPA unless the disclosure falls under the exceptions set out in section 33, including Public Interest Disclosures under section 25. Some of the reasons Employees may disclose information are (but not limited to):

i. to another public body (example: MCFD, BC Coroners Service, Parole Board of Canada) if the information is necessary for the performance of their duties;
ii. for the purpose for which the information was obtained or for a use consistent with that purpose (see section 34 of FOIPPA for “consistent use”);
iii. the head of the public body determines there is compelling circumstances that could affect anyone’s health or safety;

iv. for the purpose of reducing the risk that an individual will be a victim of domestic violence or if domestic violence is reasonably likely to occur; and
v. for a law enforcement agency (in Canada) to assist in an investigation.

4.9. Employees will take appropriate steps to verify an individual's identity before disclosing, or confirming, the individual's own Personal Information. This disclosure does not require a formal FOI request.

4.10. Individuals have the right to request records from SPS. Employees will not disclose information but will direct the individual to the Manager, Information and Privacy Unit (IPU) under SPS policy AD 9.18 *Security and Confidentiality of Records and Information – Information and Protection of Privacy Act*.

4.11. SPS has a duty under section 25 of FOIPPA to complete a Duty to Warn when there is a credible and imminent threat to life, or serious harm, to an individual. Employees will follow the guidelines in SPS policy AD 9.18 *Public Disclosures and Duty to Warn*.

4.12. SPS has a duty under section 25 of FOIPPA to complete a Public Interest Disclosure regarding a dangerous individual, or a serious incident, which could cause significant harm to a group of people. Employees will follow the guidelines in SPS policy AD 9.18 *Security and Confidentiality of Records and Information - Public Disclosure and Duty to Warn*.

FOIPPA Privacy Breach

4.13. SPS Employees who identify a Privacy Breach will report it immediately to the Manager, IPU, as well as their immediate Supervisor. The Manager, IPU must notify the Chief Constable of an unauthorized disclosure of Personal Information that is in the custody or under the control of SPS (FOIPPA section 30.5(2)).

4.14. Employees will take immediate steps to stop or contain the Privacy Breach until they can consult the Manager, IPU, who will then coordinate a containment plan and liaise with relevant units for assistance.

4.15. Employees must not alter or destroy evidence or records relating to the Privacy Breach.

4.16. The Manager, IPU will open an administrative file and may notify the SPS General Counsel, Legal Services.

4.17. The Manager, IPU will initiate an investigation and document the Privacy Breach which will include:

i. affected individuals;

ii. type of Personal Information involved;
iii. cause and extent of the Privacy Breach;
iv. containment efforts;
v. risk evaluation;
vi. notification; and
vii. prevention strategies and recommended security safeguards.

4.18. The Manager, IPU will determine whether affected parties should be notified of the Privacy Breach. Notification should be made as soon as possible and be made if the Privacy Breach will cause:

i. bodily harm, death or loss of personal property;
ii. humiliation or embarrassment;
iii. damage to reputation or relationships;
iv. loss of employment, business or professional opportunities;
v. financial loss;
vi. negative impact on credit score; or
vii. damage to, or loss of property.

4.19. The Manager, IPU will determine which Employee will carry out the notification. Notification to an affected party will be made directly whenever possible. Indirect methods can be used if the Privacy Breach affects many individuals or if those individuals' contact information is not available.

4.20. Notification should include:

i. date of the Privacy Breach;
ii. description of the Privacy Breach;
iii. description of Personal Information involved;
iv. risk(s) to the individual;
v. steps taken to control or reduce the harm;
vi. further steps planned to prevent similar Privacy Breaches;
vii. steps the individual can take to control or reduce the harm; and
viii. contact information for the Office of the Information and Privacy Commissioner (OIPC).

4.21. The Manager, IPU, in consultation with any relevant unit, will evaluate the Privacy Breach to determine steps needed to prevent a similar Privacy Breach from occurring.

4.22. The Manager, IPU will determine if SPS must notify the OIPC of the Privacy Breach.

APPENDIX A: DEFINITIONS

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

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

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

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

“Personal Information" means recorded information about an identifiable individual other than contact information.

“Privacy Breach” means the unauthorized access to Personal Information or the unauthorized collection, use, or disclosure of Personal Information in contravention of FOIPPA.

"Record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records, for the purpose of FOIPPA.

“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.

APPENDIX B: REFERENCES

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