Policy Name:	**CANADIAN POLICE INFORMATION CENTRE (CPIC) POLICY**		
Policy #:	AD 9.3	**Last Updated:**	2022-01-27
Issued By:	SUPPORT SERVICES BUREAU	**Approved By:**	SURREY POLICE BOARD
		Review Frequency:	AS REQUIRED

RELATED POLICIES

AD 9.18 *Security and Confidentiality of Records and Information*

1. PURPOSE

1.1. To ensure Surrey Police Service (SPS) Employees meet established, consistent, and authorized criteria for the use of the Canadian Police Information Centre (CPIC).

2. SCOPE

2.1. This policy applies to all SPS Employees.

3. POLICY

3.1. SPS is approved as a Category 1 CPIC Agency by the Canadian Police Information Centre (CPIC) Advisory Committee. SPS has full peace officer authority provided under the *Police Act* (primary role of the agency is law enforcement). As a Category 1 agency, SPS has full CPIC access and can perform:

i. all transaction types in the Investigative Data Bank files;
ii. query transaction in the Investigative Data Bank files;
iii. query transaction in Ancillary Data Bank files; and
iv. message transmission and reception via the CPIC telecommunications system.

3.2. Information that is contributed to, stored in, and retrieved from CPIC is supplied in confidence by the originating agency for the purpose of assisting in the detection, prevention or suppression of crime and the enforcement of law. CPIC information is to be used only for activities authorized by SPS.

CPIC Advisory Committee

3.3. The CPIC Advisory Committee approves system policy and procedural matters. This body is composed of representatives of major city police departments in Canada and Federal and Provincial law enforcement representatives.

3.4. The CPIC Advisory Committee is responsible for establishing the scope and content of CPIC data banks, how the system is used and regulated and the criteria to determine which agencies are eligible to use the system.

Access to Data Banks

3.5. SPS is responsible for the confidentiality and dissemination of information stored on the CPIC system. The dissemination of CPIC information from the SPS is at the discretion of the Chief Constable or designate and must be in accordance with existing federal and provincial policy and legislation concerning privacy and information.

3.6. SPS is under no obligation to release information but may do so in the interest of law enforcement. The CPIC Reference Manual lists agencies that are authorized to access CPIC data banks. Requests for information are restricted to sworn officers of the agencies listed in the CPIC Reference Manual.

3.7. Access to CPIC information or Network Interface (e.g., Motor Vehicle Branch) is restricted, unless authorized by the Chief Constable or designate.

3.8. CPIC Information or Network Interface information must not be disclosed to subsidiary Employees, contractors, and consultants.

3.9. The Chief Constable is ultimately responsible for SPS adherence to all policies and procedures regarding the protection and use of CPIC systems and data, including CPIC Security Standards.

4. PROCEDURE

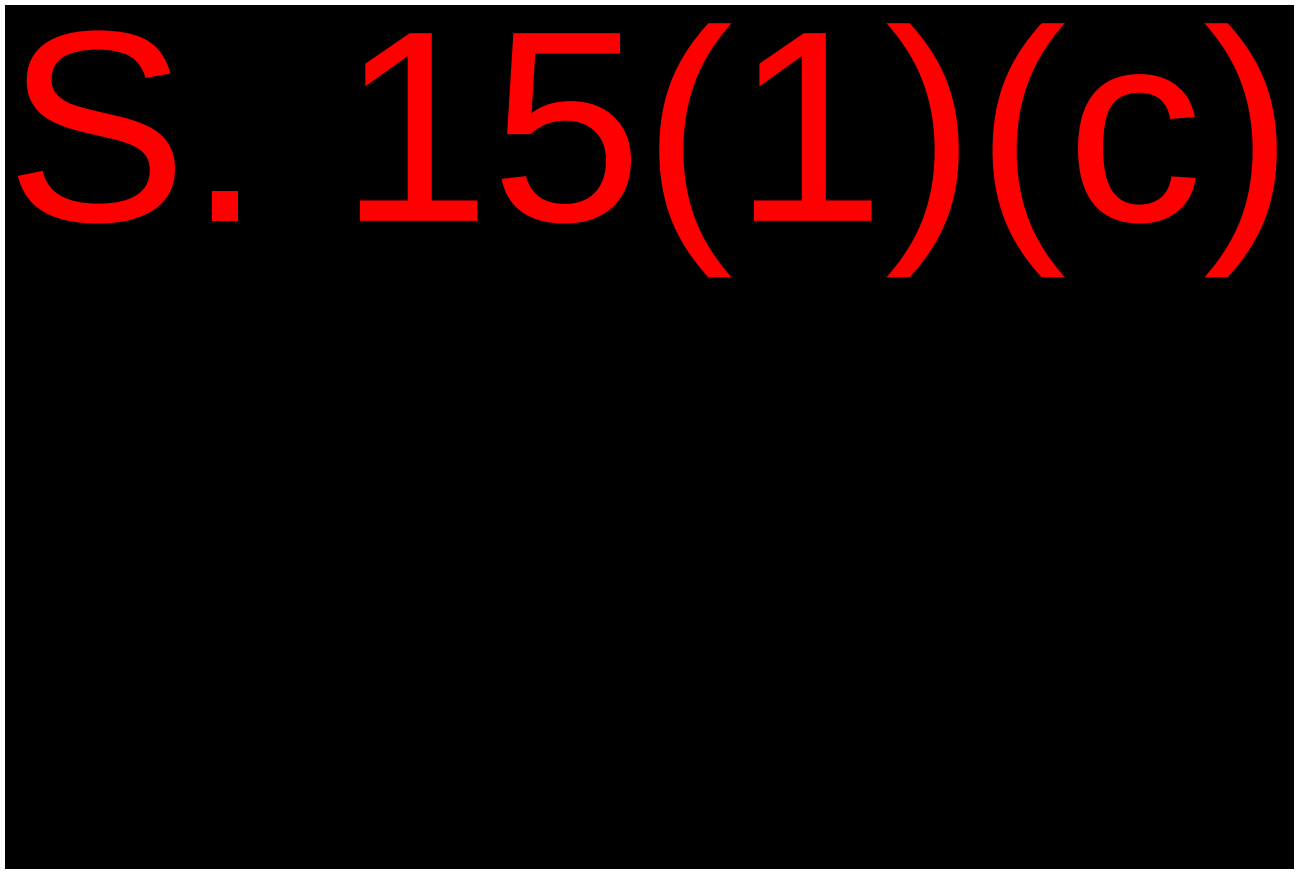
S. 15(1)(c)

[redacted]

[redacted]

Release of Information

Identification Data Bank – Criminal Record (CR)



[redacted]

Identification Data Bank – CNI/CRS

4.14. Employees must only disclose Criminal Name Index / Criminal Record Synopsis (CNI/CRS) data to authorized agencies/individuals and only for criminal or investigative purposes.

4.15. If the CPIC hard copy is to be disclosed for criminal or investigative purposes, the SPS Employee must remove CPIC CNI/CRS query format and any information not applicable to the requestor from the printout to protect the integrity of the CPIC system. The information may also be disclosed verbally or in writing.

4.16. If the request is for criminal or investigative purposes and is not accompanied by fingerprints, the Employee must provide the following caution to the requestor: "CAUTION: This record may or may not pertain to the subject of your enquiry. Positive identification can only be confirmed through the submission of fingerprints."

Police File Information

4.17. Any record placed into the CPIC system must be the subject of a police file maintained by the originator for as long as the record is on the CPIC system. Whenever a record is entered onto or removed from the CPIC system data files, such information must be contained on the PRIME General Occurrence file (GO) file.

4.18. A record placed on the CPIC system by an SPS Employee is deemed to be under SPS control. Access to that record can only be granted by SPS, under the federal/provincial access legislation that applies to that agency/department.

4.19. SPS must obtain original documents from the courts to support their CPIC Person entries; however, subject to legislation, if the document is only available via photocopy, facsimile or electronically, then the document may be used for CPIC entry purposes.

4.20. If the original court document is not available, SPS Employees must add a suitable notation to the agency file outlining the reason(s) the original document is not present on the file.

4.21. Photocopies of other reproduction of these court documents can be further disseminated under controlled circumstances and should be clearly identified as true copies.

4.22. Upon receipt of the "original copy" of an electronic document from the court, the Employee must stamp/initial/date it to indicate that it is the "original copy."

Authorization for Record Input

[redacted]
S. 15(1)(c)

[redacted]

Court Disclosure of Police Files

[redacted]
S. 15(1)(c)

4.26. Employees having direct terminal access to CPIC must complete the following requirements prior to access being permitted:

i. undergone a criminal record check;
ii. have successfully completed the CPIC mandatory course; and
iii. agree to not share their user ID, access and/or password with another person.

Unauthorized Persons

4.27. Employees must ensure that unauthorized personnel, including terminal maintenance technicians, are:

i. properly identified;
ii. accompanied by an authorized staff person (i.e., a person capable of providing assurance that no unauthorized access to data has taken place) at all times while at the SPS Workplace; and
iii. restricted to Instruction Mode transactions if operation of the terminal is required.

4.28. When it is necessary for an Employee to provide information produced from the CPIC computer system to unauthorized persons (e.g., Crown Counsel) the information must be only be in the form of a duplicate copy. All printouts that may be used or seen by other than Members and authorized personnel will have the SPS Terminal Identifiers removed and will be stamped with the following:

"Property of the Surrey Police Service. This police report is supplied to you for information of your department only. It is not to be disclosed or made known to any other agency or person without advance, written permission of the Surrey Police Service."

Access to CPIC Terminals

4.29. Members may access CPIC via Police Records Information Management Environment (PRIME) on authorized computer terminals in SPS police buildings, sub-offices and on Mobile Data Terminals (MDTs) in designated police vehicles.

Audit

4.30. The CPIC Records Section must undertake a physical audit of SPS CPIC records at least once every four (4) years.

Access to CPIC/PRIME

4.31. The Chief Constable can give access to CPIC and PRIME to designated persons and prescribe limitations to the access.

Wandering Persons Registry

4.32. The Alzheimer Society of Canada and its provincial chapters are the principal source for records entered into the Wandering Persons Registry, which is uploaded to the CPIC system.

S. 15(1)(c)

4.34. If SPS receives inquiries regarding the Alzheimer Wandering Persons Registry, registration forms are available on the Internet @ www.alzheimer.ca or from any one of the local Alzheimer of Canada chapters (the addresses of which are also available through the web site).

CPIC Retention Schedule

4.35. The expiry dates for CPIC entries are set in the CPIC Reference Manual. SPS complies with the CPIC Reference Manual retention schedule.

APPENDIX A: DEFINITIONS

"CPIC and CPIC system" means the Canadian Police Information Centre computer system, a national Police Service administered by the Royal Canadian Mounted Police (RCMP).

"CNI" means CPIC – Criminal Name Index.

"CRS" means CPIC – Criminal Record Synopsis.

"CR II" means CPIC – Criminal Record, Level II.

"Employee" means a sworn Member or Civilian Employee appointed by the Surrey Police Board.

"GO" means General Occurrence Report submitted in the PRIME records management system.

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

"PRIME" means Police Records Information Management Environment, the provincial police records management system.

"SPS" means the Surrey Police Service.

"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 the SPS.

"Workplace" means anywhere activities directly related to the business of SPS occur, including social events where there is potential for adverse effect on the workplace or any location travelled to for a work-related reason.

APPENDIX B: REFERENCES

Canadian Police Information Centre (2018). *CPIC User Manual.* Policy and Procedures Unit.

Royal Canadian Mounted Police (2019). *CPI Centre Systems Policy Manual.*