Delta Police Department
Operations Policy

AE12 PRIVATE AND INVISIBLE RECORDS AE12

Effective Date: 12 June 2014
Revised Date: 08 March 2018

POLICY

1. Users of PRIME or legacy records management systems, e.g., PIRS, may only make an entire report, a part of a report, or any other record “private” or “invisible” in accordance with criteria and authorization provisions of this policy, and will be guided by the principle that PRIME is a law enforcement information sharing tool in which only the most sensitive of information or information subject by law to non-disclosure, is to be made private or invisible.

DEFINITIONS

CAD – Computer Aided Dispatch
CCJS – Canadian Centre for Justice Statistics
CPIC – Canadian Police Information Centre
DRE – Direct Report Entry
GO – General Occurrence
JUSTIN – Justice Information Network
PIRS – Police Information Retrieval System
PRIME – Police Records Information Management Environment
RMS – Records Management System
RTCC – Report to Crown Counsel

REASON FOR POLICY

2. Making records private or invisible are powerful tools to control access to sensitive information; however, inappropriate use can have serious consequences by impeding information sharing and causing the collection of inaccurate reporting statistics or allowing access to sensitive information.

3. To comply with provincial multi-jurisdictional PRIME-BC Operational Policy and Procedures.

4. To ensure that PRIME users only make private or invisible those PRIME records or portion thereof that meet established criteria and as authorized.

5. To manage the dual priorities of protecting sensitive information, and information sharing within the Delta Police Department ("Department") and among other PRIME users agencies.

6. To ensure that users properly assess when only selected records need to be made private or invisible, and not an entire report.

- CAUTION -

7. Particular caution must be exercised in relation to the following records management system functions:

   a) CAD Call Logs: Privatizing or making a file invisible does not make information received and recorded on the CAD server private or invisible. If information needs to be removed from CAD, it must be scanned to the investigative PRIME file. Information may then be deleted from CAD and from the CAD call in RMS. The position holders authorized to approve making records private or invisible, as per this policy, may approve the deletion of CAD information by the PRIME Coordinator.

   b) Flagged Records: When adding entities on a privatized, invisible or sensitive file, be aware that if the entity is the subject of a "Flag Record" with an auto-response, whether within the Department or at another police agency, a notification will be generated that the entity has been added.

   c) Property Entries: Property entries can be privatized, but cannot be made, invisible. A property browse will reveal a property entry and may therefore compromise an invisible record.

   d) Name Queries: Name queries will identify the existence of privatized files, but also of invisible files when the number in the Events field exceeds the number of entries displayed in the Synopsis list.

e) Causing CCJS Errors: CCJS edit reports, that are required to be prepared in the Records unit, may disclose information related to private or invisible files, and care should be taken when adding or changing role codes so as not to generate a CCJS error.

f) RTCC Submissions via JUSTIN: Private or invisible records cannot be submitted via JUSTIN. When a RTCC is submitted via JUSTIN, it normally becomes available to a wide range of Crown and court system JUSTIN users. If instructed by the responsible investigator, Court Liaison can limit the Crown and court system users who will have access to a submitted RTCC. Alternatively, consideration may be given to discussing with Crown whether to submit a RTCC outside of normal JUSTIN processes.

PROCEDURES

8. Records made private in PRIME allow users who are not on the authorized access list to identify the existence of a file number and the Responsible User, while records made invisible are completely hidden from all users, except those on the access list.

9. Whenever information is made private or invisible, one of the following position holders is to be assigned as the Responsible User:

a) the investigating member;

b) the investigating member’s supervisor; or

c) any position holder authorized to approve making the report private or invisible.

Authorizing and Making a Report or a Portion thereof Private

10. The following position holders are authorized to approve making a report, a portion thereof, or any other record in PRIME or a legacy RMS, private:

a) Chief Constable;

b) Deputy Chief Constable;

c) Superintendent;

d) Inspector;

e) Staff Sergeant; and

f) Sergeant, Major Crime, Criminal Investigation Branch.

11. Any other position wishing to privatize a file must submit a request through the chain of command.

12. Any file to be privatized must be accompanied by a completed Private/Invisible File Request template text page added to the GO report and a manual NOTIFY sent to the HPRIV handle.

13. The position holders authorized to approve the privatization of information must ensure that the information meets one or more of the following criteria:

a) is hold back evidence;

b) contains sensitive or confidential investigative or third party information that is not to be known by others in the Department or at another police agency;

c) is low level or skeletal intelligence (with no national security implications);

d) relates to an investigation in which a sworn member, police staff or volunteer is a subject of the investigation (but not to include motor vehicle collision investigations unless criminal charges are anticipated to result);

e) the information could otherwise jeopardize an ongoing investigation or the safety of any person, if it were accessible to others in the Department or at another police agency; and

f) is subject to a legislated non-disclosure requirement, e.g., the *Youth Criminal Justice Act*.

14. Except as otherwise directed by the Chief Constable or a Deputy Chief Constable, the following individuals are to be granted, and only these individuals may be granted, access to a private file or record:

a) the member designated as the Responsible User;

b) the Responsible User’s supervisor;

c) individuals designated by the Responsible User or the Supervisor, including individuals at other agencies on the same PRIME server;

d) default group consisting of:

i) PRIME Coordinator and PRIME Assistant;

ii) Records Supervisor; and

iii) Criminal Investigation Branch assigned Quality Assurance Reviewer;

e) where a RTCC is to be submitted:

i) Court Liaison Unit;

f) where a CPIC entry has been attached to a PRIME file:

i) CPIC Unit; and

ii) the provincial Independent Investigations Office (by means of the HIIO handle), if it is determined by a Deputy Chief Constable or the Inspector i/c Professional Standards Branch or designate that the Office has an investigatory need to access the file.

15. The following position holders have authority to administer the change to the security of the file and make it private:

a) PRIME Coordinator and PRIME Assistant;

b) RMS System Administrator;

c) Inspector, Criminal Investigation Branch;

d) Staff Sergeant, Criminal Investigation Branch; and

e) Sergeant, Major Crime, Criminal Investigation Branch.

Authorizing and Making an Entire Report or a Portion thereof “Invisible”

16. A report made invisible in its entirety does not “exist” in PRIME, except to those who have been given access to it. Readers will not be able to transcribe any supplementary information to a report made invisible in its entirety. Considerations should be given to submitting supplementary reports only through DRE by those who have access to the file, thus eliminating the transcription queue. If only a portion of a report is made invisible the report will be accessible by all users except for the part of the report that was made invisible.

17. Only an Inspector or position of higher rank may authorize a report or portion thereof to be made invisible.

18. Those authorized to have a report or portion thereof made invisible must ensure that the information meets one or more of the following criteria:

    a) involves a sworn or police staff employee of the Department;

    b) is confidential or source information, which if compromised may endanger a person’s life, or

    c) is extremely sensitive intelligence information.

19. Any other report or information may be made invisible only if approved by a Deputy Chief Constable or the Chief Constable.

20. Except as otherwise directed by the Chief Constable or a Deputy Chief Constable, the following individuals are to be granted, and only these individuals may be granted, access to an invisible file or record:

    a) the member designated as the Responsible User;

    b) the Responsible User’s Supervisor;

    c) the approving Inspector;

    d) those records management staff authorized by the approving Inspector;

    e) the provincial Independent Investigations Office (by means of the HIIO handle), if it is determined by a Deputy Chief Constable, or the Inspector i/c Professional Standards Branch or designate, that the Office has an investigatory need to access the file; and

f) any other position holders considered necessary by the approving Inspector.

21. Whenever an entire report or portion thereof is made invisible, the Responsible User must notify the PRIME Coordinator of the fact by completing a Private/Invisible File Request template text page, adding it to the GO and sending a manual NOTIFY to the HPRIV handle.

22. The following position holders have authority to administer the change to the security of the file and make it invisible:

a) PRIME Coordinator and PRIME Assistant;

b) PIRS System Administrator;

c) Inspector, Criminal Investigation Branch;

d) Staff Sergeant, Criminal Investigation Branch.

RTCC Submissions

23. Before charges are forwarded to Crown Counsel, the Responsible User will review the file to determine the need to maintain the classification, and to determine what viewer access restrictions on the Crown and Courts side, if any, are required to be implemented in the JUSTIN submission process.

Access for FOI Requests

24. The approving Officer may grant the Chief Constable's designates under the *Freedom of Information and Protection of Privacy Act*, access to a private or invisible file, in order to enable the Department to comply with the requirements of that *Act*.

Review of File Status

25. If the Responsible User of a private or invisible file is transferred, retires, or is otherwise relieved of the file responsibility, the newly assigned member will review the information in the file to ensure that it still meets the requirements for being private or invisible, and the file updated to indicate the new Responsible User.

26. Before a file is closed, the Records Supervisor, in consultation with the Responsible User will ensure that the criteria to classify the file private or invisible still exist, and if the criteria are no longer met, the file will be unclassified.

27. The PRIME Coordinator will issue an annual request to all Responsible Users of private and invisible files directing that they be reviewed to determine the need to maintain their status and Responsible Users will report back to the PRIME Coordinator.

28. The approving Officer or PRIME Coordinator, upon the annual review, must record in the GO the authorization to continue or discontinue the private or invisible classification.

Hardcopy Materials Management

29. Hardcopy materials associated to a privatized or invisible file will be maintained as follows:

    a) kept in a locked cabinet in the Information Services Branch or Criminal Investigation Branch, with access by those position holders granted file access as per this policy; and

    b) active CPIC entries are to be stored in the Information Services Section to allow 24/7 access.