Policy Name:	**DIGITAL EVIDENCE MANAGEMENT**		
Policy #:	OP 5.1.2	**Last Updated:**	2023-09-27
Issued By:	SUPPORT SERVICES BUREAU	**Approved By:**	SURREY POLICE BOARD
Version:	2.0	**Review Frequency:**	AS REQUIRED

RELATED POLICIES

OP 4.15 Cyber and Technology Crimes

OP 5.1 Seized Property

OP 5.2 Retention of Property for Court Purposes (Form 5.2)

1. PURPOSE

1.1. To outline procedures for Surrey Police Service (SPS) Members to follow for seizing and managing video, audio, digital data, electronic devices, and digital media for potential evidence of a crime and to prevent destruction of this evidence.

1.2. To establish policy and procedures for the use of the SPS Digital Evidence Management System (DEMS)

1.3. To outline Member's legal authorities when seizing electronic devices and/or cameras from individual observers at crime scenes.

1.4. To outline procedures for properly viewing, seizing, handling, storing and maintaining continuity of digital media and data to ensure its integrity and admissibility for potential court purposes.

2. SCOPE

2.1. This policy applies to all SPS Employees.

3. POLICY

3.1. Members may be required to seize electronic devices from persons that are believed to contain images, audio, and/or photographs that are evidence of a crime and /or collect / capture information from person(s) or location(s).

3.2. Members may be required to view and/or seize video evidence of a crime that has been captured on video surveillance equipment and stored on a digital video recorder (DVR).

3.3. When considering the seizure of electronic devices in these situations, Members must ensure that the seizure is both lawful and reasonable. Members must understand the legal authorities that allow them to seize digital evidence:

i. with consent from the owner;
ii. incidental to lawful arrest;
iii. pursuant to a general search warrant under section 487 of the *Criminal Code*;
iv. without a warrant under "exigent circumstances" as authorized under section 487.11 of the *Criminal Code*:
    a. "Exigent Circumstances" (for the purposes of this policy) are circumstances where a Member must immediately act to protect public safety and/or prevent the imminent destruction of evidence and preserve evidence of a crime. This includes the seizure of an individual's electronic device or camera without a warrant; and
    b. To seize an electronic device or camera under "exigent circumstances", the Member must have grounds for obtaining a warrant but it would be impracticable to obtain a warrant (e.g., the Member has reasonable grounds to believe that the video or digital media evidence will be lost or destroyed while a warrant is being obtained).

3.4. The Digital Forensics Unit (DFU) is responsible for recovering and seizing digital evidence from electronic devices using specialized software.

3.5. DFU can assist Members with safely extracting and securing video footage from digital video recording equipment and making copies of video and audio files for court purposes.

4. PROCEDURE

Seizing of Electronic Devices or Cameras from Individuals

4.1. While at a crime scene, if a Member observes individuals (who are *not* suspects in the matter under investigation) using an electronic device (including a camera) to take photographs and/or record video and/or audio, and if the Member has reasonable grounds to believe that evidence may have been captured on the electronic device, the Member will:

i. ask the individual for consent to seize and search their electronic device for evidence;
ii. if the individual does not consent to the seizure and search of their device, ask the individual to provide their name, phone number and address where they can be served with a warrant;

iii. attempt to determine if there are any concerns that the individual will not be located to receive service of the warrant, or if the individual may destroy or lose the evidence or device prior to the warrant being served;
iv. if the individual agrees to a consent search of their electronic device, have them sign an Authorization for Consent Search which clearly states what the device will be searched for and their right to be present during the search and to stop the search at any time (i.e., ensure that they are providing "informed consent"). Obtain the password for the device if necessary;
v. if the Member believes that the individual may not later be located, or that the individual may destroy or lose the evidence or device, seize the electronic device under "exigent circumstances";
vi. explain to the individual the police's legal authority under section 487.11 of the *Criminal Code* to seize the electronic device; and
vii. provide the individual with the police file number along with the Member's name and contact information (a work telephone number and email address).

4.2. When seizing an electronic device, a Member must:

i. record the physical description including make, model, colour, serial number, and/or any other unique descriptors of the electronic device in their notebook;
ii. if the electronic device is a cellular phone:
    a. do not attempt to unlock the phone or check any incoming or outgoing messages;
    b. attach an external battery charger as soon as practicable;
    c. if the device is powered on, do not turn it off;
    d. if the device is powered off, do not turn on the power as it may allow access into the device to erase its contents; and
    e. secure the electronic device in a radio frequency proof receptacle (e.g., Faraday bag or metal container);
iii. create a PRIME-BC report to record the circumstances of the incident and further investigative steps (e.g., drafting of a warrant to search the electronic device). If the electronic device was seized under "exigent circumstances", clearly articulate the legal authorities, grounds for, and circumstances of the seizure;
iv. enter details for the seized electronic device into the PRIME-BC GO property module;
v. complete Form PCR 087 (Report to a Justice Form 5.2) to detain the seized electronic device for 90 days, and request a diary date to prepare an extension of the 5.2;
vi. Regular Hours:
    a. contact the DFU for assistance and notify them of the presence of digital evidence on the electronic device;
    b. transport the seized electronic device to the DFU for secure storage; and
    c. if consent was obtained, provide them with a copy of the signed Consent to Search and if no consent was obtained, tell them that a warrant will be sought;
vii. After Hours:
    a. store the seized electronic device in a secure locker at the Property Office or in a secure locker specifically assigned to the Digital Forensics Unit; and

b. enter a Miscellaneous Notes (MN) page in the PRIME-BC GO report requesting digital forensic examination of the electronic device and explaining the authority for the examination (e.g., consent or warrant).

4.3. If consent was not obtained from the device's owner to search the device but the device needs to be searched to advance the investigation, obtain the appropriate judicial authorization to search the electronic device, to be executed by the DFU:

i. record details of all digital media evidence recovered by the DFU;
ii. maintain responsibility for the electronic device, including the preparation of a Form 5.2 extension request, if a Report to Crown Counsel (RTCC) will not be sent to Crown for charge assessment within 90 days; and
iii. if an RTCC will be submitted, include a copy of the recovered digital media evidence supporting the criminal charges in the disclosure package.

Seizing of Video and/or a Digital Video Recorder (DVR)

4.4. If a Member observes the presence of video surveillance cameras or closed-circuit television (CCTV) cameras while at or near a crime scene and has reasonable grounds to believe that evidence may have been captured by the cameras and stored on a digital video recorder, Members must:

i. if the camera is in a location where a suspect would have no expectation of privacy (e.g., a shopping mall), attempt to contact the owner or authorized representative for the operation of the cameras and ask to review the video footage for evidence of a crime;
ii. upon viewing video that is evidence of a crime:
    a. request that the owner or person responsible for the operation of the camera/DVR download a copy of the video onto a DVD, USB flash drive, or other suitable media storage device;
    b. ensure that the video extracted from the DVR is in the original format and is not altered or corrupted during the extraction process;
    c. contact the DFU for assistance if the owner or person responsible for the operation of the camera/DVR is unsure how to extract the video. An DFU Member may be required to attend the scene and assist with the video extraction; and
    d. determine how long the video will be stored on the DVR before it will be overwritten, if a warrant is required;
iii. record these details:
    a. the make and model of the DVR and camera system;
    b. the date and timestamp of the video and any discrepancy between real time and the video timestamp;
    c. the name and contact information of the owner or authorized representative for the camera/DVR and their level of knowledge and expertise of the camera/DVR (if they extracted the video);

d. the name of the DFU Member who assisted with the video extraction, if applicable;
e. the date and time of a search warrant execution if applicable; and
f. how the Member ensured the continuity and preservation of the video after its extraction; and

iv. if the video was extracted by a representative of the business, obtain a brief audio statement from the representative in which they should explain their role with the business, explain any time discrepancies, and confirming that the video was not altered in any way prior to its extraction.

4.5. When a Member has seized a media storage device containing the extracted video, the Member must:

i. transport the media storage device to the Property Office for secure storage;
ii. create a PRIME-BC report outlining the circumstances of the incident and seizure of video (articulating the seizure via consent, search warrant or exigent circumstances);
iii. enter the DVD or USB flash drive containing the video into the PRIME-BC GO property module;
iv. print a property tag sticker and attach it to the outer exhibit envelope or bag containing the DVD or USB flash drive for secure storage at the Property Office; and
v. contact the DFU to properly make copies of the video for court purposes.

4.6. If the video from a DVR cannot be extracted for any reason and the Member is concerned about the loss or destruction of evidence, or if the camera is in a place where a suspect may have an expectation of privacy (e.g., an apartment building), the Member must seize the DVR, if appropriate. If the suspect may have an expectation of privacy, ensure that a warrant or production order is obtained before the device is searched.

4.7. If the Member determines that the DVR is to be seized, the Member must know their legal authorities listed above. The Member will contact a Member from DFU to assist with the seizure because the physical DVR could be damaged if powered off incorrectly, resulting in the loss or corruption of video evidence in the DVR.

4.8. When a Member has seized a DVR, the Member will follow the procedures in this policy and notify the DFU to assist with extraction of the required video evidence. If the entire DVR is seized, a Form PCR 087 (Report to Justice 5.2) will be completed. If the DVR will not be returned to the owner within 90 days, a 5.2 extension will be required.

Child Pornography

4.9. A Member who locates images or videos of child pornography on an electronic device must ensure that the electronic device is carefully handled to maintain the integrity of the evidence while ensuring that no one else is unnecessarily exposed to the images or video.

4.10. The Member will immediately stop viewing the child pornography material and notify an NCO of the Internet Child Exploitation (ICE) Team upon the discovery of the material.

4.11. The Member will seize the electronic device as per the procedures listed above and route the original PRIME-BC GO report to ICE who will take responsibility of any further investigation (see OP 4.15 *Cyber and Technology Crimes*).

Video and Audio Interviews

4.12. All original video and/or audio files of interviews conducted with suspects, victims or witnesses must be recorded and saved onto a DVD or USB flash drive or other suitable media storage device and transported to the Property Office for secure storage as per the procedures listed above.

4.13. If copies of the video and/or audio files of the interview(s) are required for court purposes, Members will request the assistance of the DFU to make the necessary copies.

4.14. Members will forward a copy of the video and/or audio files of the interview to the Typing Resource Centre to transcribe the interview for disclosure and court purposes.

4.15. Members will forward all copies of the video and/or audio files of the interview and copies of the interview transcript to the Court Liaison Clerk for disclosure to Crown Counsel.

4.16. Members will record their actions relating to audio/video recorded statements in their notebooks and on the investigative file.

Digital Forensics Unit (DFU) Responsibilities

4.17. DFU Members are responsible for:

i. reviewing authorizations (consent or warrant) to search devices, and in the case of a warrant, executing the warrant in accordance with its terms and conditions;
ii. analyzing the seized electronic device and recovering and seizing/securing the digital data;
iii. maintaining an original copy of the digital data recovered and providing the primary investigator with another copy of the digital data for the investigation;
iv. completing a detailed report outlining the investigation and providing the report to the lead investigator in a timely manner; and
v. transporting the electronic device to the Property Office for secure storage or returning the electronic device to the primary investigator who will secure the exhibit at the Property Office.
vi. assisting Members with the extraction and seizure of video from digital video recorders;
vii. attending the scene if requested by Members and if safe to do so, assisting with extracting video or seizing DVR equipment;
viii. copying seized video and audio files for disclosure and court purposes; and

ix. ensuring the integrity of all extracted and seized video and audio files and DVR equipment when handled.

Property Office Responsibilities

4.18. The Property Office will manage the storage of all electronic devices and video/audio files that are securely stored for investigation and safekeeping.

4.19. The Property Office will not return any electronic device to the owner/possessor of the electronic device without the appropriate authorization for the circumstances. For example, digital devices seized with consent from a witness may be returned at the direction of the lead investigator. However, a device seized from an accused person charged with an offence may require a valid Order To Return Things Seized that has been signed by a Justice of the Peace.

4.20. All electronic devices must be held at the Property Office for thirty-one (31) days from the date any Order is issued by a Justice of the Peace. The thirty-one (31) day period allows for appeals and disputes related to the property.

4.21. If the Property Office does not receive notification of an appeal or dispute regarding the property in question, the Property Office will follow the instructions in the Order issued by the Justice of the Peace.

Digital Evidence Management System (DEMS)

4.22. Not all digital evidence can be uploaded on the DEMS platform, in these instances, Employees will follow the processes set out in s. 4.2.

4.23. Members are provided an SPS-issue mobile device capable of capturing photographs, audio recordings and video recordings using a designated mobile application.

4.24. Members will capture photographs, audio recordings and video recordings, as appropriate to the circumstances, with SPS-issue:

i. specialty equipment assigned to the unit;
ii. Mobile devices, using the mobile application; or
iii. Video recording equipment installed in SPS interview rooms.

4.25. In Exigent Circumstances (e.g., the immediate need to preserve evidence or to share evidence with another law enforcement agency while in the field) digital evidence may be captured with non-SPS issue equipment and/or applications if SPS-issue equipment is unavailable or non-functional.

4.26. Digital evidence captured or obtained by SPS during an investigation, including material which may be duplicative, out-of-focus or inaudible must be uploaded to the DEMS. No files may be deleted prior to upload.

4.27. Media captured unintentionally and clearly unrelated to an investigation (for example, accidental audio or video recording of a personal conversation between co-workers, photographs taken of the inside of the employee's pocket) may be selectively deleted from the mobile application with the approval of the Employee's Supervisor prior to upload. The Employee and Supervisor will document the circumstances of any unintentionally captured file deletion in their police notebooks. The notes will not be associated to a police file.

4.28. An Employee uploading digital evidence to the DEMS, whether through the application or via manual upload, is responsible for associating the uploaded file(s) to a General Occurrence (GO) number and adding applicable standard naming conventions and descriptors to the file.

4.29. Unless there is an equipment malfunction or exigent circumstances that prevent immediate uploading of digital evidence to DEMS, Employees who have captured digital evidence via a mobile device must upload the files to the DEMS as soon as practicable, but by no later than the end of their shift.

4.30. An Employee who deems that the size, number or nature of digital evidence captured or obtained renders upload to DEMS not possible or unsuitable, is to seek direction from their Supervisor.

Deletion of Digital Evidence

4.31. Digital evidence uploaded to the DEMS will only be deleted in accordance with minimum retention and deletion standards set by SPS and/or PRIME-BC, and specific to file and/or offence type. The deletion of digital evidence outside of this deletion protocol is prohibited.

4.32. Employees responsible for the upload of evidence from portable storage devices (including SLR camera cards and USB thumb drives) to the DEMS may delete files from the portable device once the upload is complete and confirmed successful.

Editing Digital Evidence

4.33. The ability to edit file attributes in DEMS is determined by the DEMS role assigned to each User.

4.34. Creating extracted copies of photographs, audio recordings and video recordings using the DEMS functionality is permitted, but the original item must remain associated to the GO and may not be deleted from the DEMS outside of the deletion protocol noted above in s. 4.31 and s. 4.32.

Accessing, Sharing and Reassigning Digital Evidence

4.35. User registration with secure login is required to access the mobile application and the DEMS desktop. Access to individual items of evidence is based on the User's role.

4.36. Access to the DEMS is only permitted during the course of duties, via the use of SPS devices.

4.37. The Member who is responsible for the Digital Evidence, or a Supervisor, may re-assign evidence ownership from one DEMS User to another.

4.38. Evidence and logs in the DEMS may be shared with individuals or organizations outside SPS, subject to applicable disclosure laws, SPS policy and the terms of file-sharing agreements, where they exist.

4.39. Digital Evidence stored in the DEMS must be shared internally using the DEMS evidence sharing functionality. Digital Evidence may only be shared internally by text or email in exigent circumstances, and when access to the DEMS desktop is not available.

4.40. Only the Manager, Information and Privacy or their delegate may authorize the release of Digital Evidence under a *Freedom of Information and Protection of Privacy Act* request.

4.41. Only the Manager, Information and Privacy or their delegate may authorize the release of Digital Evidence to Crown Counsel.

4.42. Employees may share digital evidence with other Canadian law enforcement agencies.

Audit Log

4.43. DEMS maintains an audit log of all User activity. Program access and evidence uploaded, viewed, edited, deleted and shared is tracked.

4.44. The DEMS audit log is retained in perpetuity.

APPENDIX A: DEFINITIONS

"Child Pornography" means

a) photographic, film, video, or other visual representation, whether it was made by electronic or mechanical means:
   - that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or
   - the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;

b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under section 163(1) of the *Criminal Code*;

c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under section 163(1) of the *Criminal Code*; or

d) any audio recording that has as its dominant characteristic the description, presentation, or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under section 163(1) of the *Criminal Code*.

"Form 5.2" means a Form 5.2 Report to a Justice to record seizures under the *Criminal Code*, section 489.1. This section requires that where a peace officer seizes anything during the execution of their duties where either ownership is in dispute or the continued detention of the thing seized is required for the purposes of any investigation or court proceedings, the peace officer will report the items seized to a justice using a Form 5.2.

"Digital Evidence Management System" (DEMS) means the designated third-party service provider storing, securing and managing access to SPS's digital evidence.

"DFU" means the SPS Digital Forensics Unit.

"Digital and Electronic Devices" means, but is not limited to, computers, hard drives, tablets, cellular devices, other mobile devices, and electronic storage media including CD/DVDs, USB thumb drives, memory cards, and digital cameras.

"Digital Evidence" means digital photographs, audio recordings and video recordings captured or obtained by SPS during a police investigation.

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

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

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

“Mobile Application” means the SPS-designated mobile application used to facilitate the capture via mobile phone of photographs, audio statements and video statements related to police investigations, and the upload of these files to SPS’s digital evidence management system.

“PRIME-BC” means the Police Records Information Management Environment, the provincial police records management system.

“RTCC” means an investigational file with multiple reports, pages and notes sent through Police Crown Liaison to Crown Counsel for charge assessment.

“SPS” means Surrey Police Service.

“Supervisor” means a Team Leader, Manager, Staff Sergeant, 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.

"User" means an SPS Employee authorized to access the Digital Evidence Management System.

APPENDIX B: REFERENCES

Criminal Code, R.S.C. 1985, c. C-46