Appendix A

*St. Anthony Police Department Principles and Practices Manual

30-0 Portable Audio/Video Recorders

30-1 PURPOSE AND SCOPE
This policy provides guidelines for the use of portable audio/video recording devices by members of this department while in the performance of their duties (Minn. Stat. § 626.8473). Portable audio/video recording devices include all recording systems whether body-worn, handheld or integrated into portable equipment.

This policy does not apply to mobile audio/video recordings, interviews or interrogations conducted at any St. Anthony Police Department facility, undercover operations, wiretaps or eavesdropping (concealed listening devices) unless captured by a portable recording system.

30-1-1 DEFINITIONS
Definitions related to this policy include:

Portable recording system - A device worn by a member that is capable of both video and audio recording of the member's activities and interactions with others or collecting digital multimedia evidence as part of an investigation and as provided in Minn. Stat. § 13.825.

30-2 POLICY
The St. Anthony Police Department may provide members with access to portable recorders for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Department by accurately capturing contacts between members of the Department and the public.

30-2-1 MOBILE VIDEO RECORDER OBJECTIVES
The St. Anthony Police Department has adopted the use of portable audio/video recorders to accomplish the following objectives:

(a) To enhance officer safety.
(b) To document statements and events during the course of an incident.
(c) To enhance the officer's ability to document and review statements and actions for both internal reporting requirements and for courtroom preparation/presentation.
(d) To preserve audio and visual information for use in current and future investigations.
(e) To provide a tool for self-critique and field evaluation during officer training.
(f) To enhance the public trust by preserving factual representations of officer-citizen interactions in the form of audio-video recordings.
(g) To assist with the defense of civil actions against law enforcement officers and the City of St. Anthony.
(h) To assist with the training and evaluation of officers.

30-3 MEMBER RESPONSIBILITIES
Prior to going into service, each uniformed member will be responsible for making sure that he/she is equipped with a portable recorder issued by the Department, and that the recorder is in good working

order (Minn. Stat. § 13.825). If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner or otherwise notify persons that they are being recorded, whenever reasonably practicable (Minn. Stat. § 626.8473).

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

When using a portable recorder, the assigned member shall record his/her name, employee number and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording.

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording (Minn. Stat. § 626.8473). Members should include the reason for deactivation.

30-3-1 SPARE DEVICES
When using a spare device, or one that is not assigned to the member, it is the member's responsibility to notify the supervisor on duty of the reason they are unable to use their issued equipment. In addition, it is the member's responsibility to notify the Records Supervisor to ensure the evidence that was recorded on that device can be reassigned to the recording member in the Back End Client software.

30-4 SUPERVISOR RESPONSIBILITIES
Supervisors shall ensure officers are using their portable audio/video recorders per policy. Supervisors should determine corrective action for non-functioning portable audio/video recorders. When an incident arises that requires the immediate retrieval of the recorded media (e.g., serious crime scenes, peace officer-involved shootings, department-involved collisions), a supervisor shall ensure that the portable audio/video recorders are properly uploaded.

30-5 ADMINISTRATOR RESPONSIBILITIES
The portable audio/video recorder administrator (designated personnel authorized by the Chief of Police) are responsible for deleting media:

(a) Pursuant to a court order.
(b) In accordance with established records retention policies, including reissuing all other media deemed to be of no evidentiary value.
(c) In instances where privacy issues are noted and no evidentiary value exists.
(d) Ordering, issuing, retrieving and storing all portable audio/video recorders.
(e) Logs reflecting portable audio/video recorder assignments, serial number, the date it was issued, and the officer to which it was issued.

30-6 COORDINATOR

The Chief of Police or the authorized designee should designate a coordinator responsible for (Minn. Stat. § 626.8473; Minn. Stat. § 13.825):

(a) Establishing procedures for the security, storage and maintenance of data and recordings.
    1. The coordinator (Services Manager) should work with the Custodian of Records (Records Supervisor) and the member assigned to coordinate the use, access and release of protected information to ensure that procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) and other applicable laws (Minn. Stat. § 13.01 et seq.) (See the Standards of Conduct Policy, Principles 2 and 8, and the Maintenance and Disclosure of Data Policy 13-7)

(b) Establishing procedures for accessing data and recordings.
    1. These procedures should include the process to obtain written authorization for access to non-public data by SAPD members and members of other governmental entities and agencies.

(c) Establishing procedures for logging or auditing access.

(d) Establishing procedures for transferring, downloading, tagging or marking events.

(e) Establishing an inventory of portable recorders including:
    1. Total number of devices owned or maintained by the St. Anthony Police Department.
    2. Daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used.
    3. Total amount of recorded audio and video data collected by the devices and maintained by the St. Anthony Police Department.

(f) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.

(g) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the St. Anthony Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.

30-7 ACTIVATION OF THE AUDIO/VIDEO RECORDER

This policy is not intended to describe every possible situation in which the recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

The recorder should be activated in any of the following situations:

(a) All enforcement and investigative contacts including stops and field interview (FI) situations
(b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops
(c) Self-initiated activity in which a member would normally notify the Hennepin County or Ramsey County Communications Dispatch Centers.
(d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording.

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is a member expected to jeopardize his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

30-7-1 CESSATION OF RECORDING

Once activated, the portable recorder should usually remain on continuously until the member reasonably believes that his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation.

Recording may be temporarily ceased or the audio muted to exchange information with other officers, legal counsel, or the lens obstructed in order to avoid capturing images of undercover officers, informants, or citizens where based on training and experience, in the judgement of the officer a recording would not be appropriate or consistent with this policy. The reason to cease and resume recording (or to mute audio or obstruct the lens) will be noted by the officer either verbally on the portable audio/video recorder or in a written report.

Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.

Formal statements recorded on portable audio/video recorders shall be recorded as separate recordings. Recordings shall be categorized, titled and identified in accordance with established policies and procedures.

30-7-2 WHEN ACTIVATION IS NOT REQUIRED

Activation of the portable audio/video recorder system is not required:

(a) During encounters with undercover officers or informants.
(b) When an officer is on break or is otherwise engaged in personal activities.
(c) In any location where individuals have a reasonable expectation of privacy, such as a restroom, locker room or break room.
(d) When not in service or actively on patrol.

30-7-3 SURREPTITIOUS RECORDINGS

Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Minn. Stat. § 626A.02).

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee.

30-8 REVIEW OF RECORDED MEDIA FILES

When preparing written reports, members are permitted to review their recordings as a resource (See the Officer-Involved Shootings and Deaths Policy 9-28 for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

(a) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation or criminal investigation.
(b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.
(c) In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy 8-1.

Officers shall document in the Post Note field of the Back End Client software the purpose for accessing any recorded file. This documentation is to clarify the reason for viewing the recording when developing the audit trail.

All recordings should be reviewed by the Custodian of Records (Records Supervisor) prior to public release (See the Records Maintenance and Release Policy 8-1). Recordings that are clearly offensive to common sensibilities should not be publicly released unless disclosure is required by law or order of the court (Minn. Stat. § 13.82, Subd. 7).

30-9 RECORDING MEDIA STORAGE AND INTEGRITY

At the end of their shift, officers shall place the portable audio/video recorder into the docking station. This will allow the data to be transferred from the audio/video recorder through the docking station to Arbitrator Back End Client. The data is considered impounded at this point and the portable audio/video recorder is cleared of existing data. The portable audio/video recorder should not be removed from the docking station until the data has been uploaded and the battery has been fully recharged.

30-9-1 COPIES OF RECORDING MEDIA

Evidentiary copies of digital recordings will be accessed and copied from the Back End Client software for official law enforcement purposes only. Access rights may be given to the Hennepin County Attorney, Ramsey County Attorney, St. Anthony, Lauderdale and Falcon Heights City Attorney's, or other prosecutorial agencies associated with any future prosecution arising from an incident in which the portable audio/video recorder was utilized.

Officers shall ensure relevant recordings are preserved. Officers or portable audio/video recorder administrators may prevent automatic deletion by changing the category of the media at any time prior to deletion.

30-10 SYSTEM OPERATIONAL STANDARDS

(a) Portable audio/video recorder system use should be based on officer safety requirements and device manufacturer recommendations.

(b) The portable audio/video recorder system should be configured to minimally buffer for 30 seconds prior to activation.

(c) For each digital recording, officers shall select the proper category. Members shall enter the 8-digit case file number or the full citation number and descriptive title. The title should clearly describe the nature of the recording. For example:

1. Initial Contact (if use of force was used, add UOF)
2. Booking
3. Transport (if The Wrap was used, add Wrap)
4. Impound
5. Narr (narrative report)
6. IC Jane Doe (implied consent)
7. SS John Doe (suspect statement)
8. VS Jane Doe (victim statement)
9. WS Jane Doe (witness statement)
10. Telephone Call with John Doe

(d) Digital recordings shall be retained according to the Department's retention schedule or as required by the rules of evidence, unless a specific request is made to store them for a longer period of time by an authorized person.

(e) Members shall not attempt to delete, alter, reuse, modify or tamper with portable audio/video recorder systems or recordings.

30-11 CLASSIFICATION OF MVR DATA

Nothing in this policy shall be interpreted as changing the underlying classification of data collected by portable audio/video recorder systems. The classification of data collected by portable audio/ video recorder systems will need to be determined on a case-by-case basis upon application and interpretation of the MGDPA and other laws.

30-12 PROHIBITED USE OF AUDIO/VIDEO RECORDERS

Members are prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with department-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department.

Members are prohibited from using personally owned recording devices while on-duty without the express consent of the on duty supervisor or OIC. Any member who uses a personally owned recorder for department-related activities shall comply with the provisions of this policy, including retention and

release requirements and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

30-13 RETENTION OF RECORDINGS
All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 90 days, except as provided in accordance with the Minnesota Data Practices Act.

If an individual captured in a recording submits a written request, the recording may be retained for an additional time period. The coordinator should be responsible for notifying the individual prior to destruction of the recording (Minn. Stat. § 13.825).

30-13-1 RELEASE OF AUDIO/VIDEO RECORDINGS
Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release and Disclosure of Data Policies.

30-13-2 ACCESS TO RECORDINGS

Except as provided by Minn. Stat. § 13.825, Subd. 2, audio/video recordings are considered private or nonpublic data.

Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have the consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the subject unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17.

30-14 ACCOUNTABILITY
Any member who accesses or releases recordings without authorization may be subject to discipline (See the Standards of Conduct Policy 4-0, Principle 2 and 8 and the Maintenance and Disclosure of Data Policy 13-7) (Minn. Stat. §626.8473).

30-15 SANCTIONS FOR MISUSE OF RECORDED MEDIA
Any member misusing recorded media for other than official law enforcement purposes will be subject to disciplinary action.

The Chief of Police, or designee, shall meet with the person who is alleged to have violated the policy and determine appropriate sanctions, which may include any or all of the standard discipline policies currently in place at the St. Anthony Police Department including verbal reprimand, written reprimand, suspension or termination. Intentional misuse of recorded media is a serious violation. If criminal behavior is believed to have occurred, appropriate agencies will be notified for further investigation.

The specific situation in each case of misuse of recorded media will be looked at with all circumstances considered when determining disciplinary actions. Consideration will be given to the extent of the loss or injury to the system, agency, or other person upon release or disclosure of sensitive or classified information to an unauthorized individual.

30-16 TRAINING

Users of the MVR systems and supervisors shall successfully complete an approved course of instruction prior to being deployed. This training shall be documented by the Supervisor in charge of training.

Appendix B

SAPD Policy 9-28 (Officer-Involved Shootings and Deaths), Interviews, places limitations on an officer's ability to view recordings prior to offering a statement or writing a report. Policy falls in line with the MN BCA policy regarding the investigation of an officer-involved shooting.

- When an Investigative Agent is taking a statement from a St. Anthony Police Officer who used or attempted to use deadly force in a critical incident and the incident is captured on video or audio recordings, the following process should normally take place:

    I. The peace officer will be requested to provide a voluntary interview of the facts and circumstances surrounding the incident.
    II. Neither the officer nor their attorney will be permitted to view the video prior to providing a voluntary statement. However, a peace officer may view the video following the voluntary interview if they request to do so to assist in clarifying any portion of their statement. The viewing of the video will be limited to the incident captured on the officer's own dash camera or BWC.
    III. If the peace officer requests to view the video, they will be afforded an opportunity to do so at the conclusion of the voluntary statement. The Investigative Agent should make arrangements to show the video as soon as feasible following the statement. Investigative personnel should be present for the viewing of the video and the officer's legal representation may be present as well. No other persons, other than people needed for technical assistance, should be present for the viewing of this video.
    IV. If multiple cameras from other sources captured the incident, the Investigative Agent shall determine if additional video should be shown to the involved officer on a case by case basis.
    V. At the conclusion of the viewing of this video, the peace officer shall be afforded the opportunity to consult privately with their attorney.
    VI. Once such consultation has occurred, the Investigative Agent shall provide an opportunity to the involved peace officer to clarify any portions of their statement after viewing the video.

Appendix C

M.S.S. 626.8473 PORTABLE RECORDING SYSTEMS ADOPTION; WRITTEN POLICY REQUIRED. *

Subdivision 1. Definition. As used in this section, "portable recording system" has the meaning provided in section 13.825, subdivision 1.

Subd. 2. Public comment. A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly scheduled meeting.

Subd. 3. Written policies and procedures required.

(a) The chief officer of every state and local law enforcement agency that uses or proposes to use a portable recording system must establish and enforce a written policy governing its use. In developing and adopting the policy, the law enforcement agency must provide for public comment and input as provided in subdivision 2. Use of a portable recording system without adoption of a written policy meeting the requirements of this section is prohibited. The written policy must be posted on the agency's Web site, if the agency has a Web site.

(b) At a minimum, the written policy must incorporate the following:

(1) the requirements of section 13.825 and other data classifications, access procedures, retention policies, and data security safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;

(2) procedures for testing the portable recording system to ensure adequate functioning;

(3) procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;

(4) circumstances under which recording is mandatory, prohibited, or at the discretion of the officer using the system;

(5) circumstances under which a data subject must be given notice of a recording;

(6) circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;

(7) procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and

(8) procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

Appendix D

M.S.S. 13.825 PORTABLE RECORDING SYSTEMS.

Subdivision 1. Application; definition.

(a) This section applies to law enforcement agencies that maintain a portable recording system for use in investigations, or in response to emergencies, incidents, and requests for service.

(b) As used in this section:

(1) "portable recording system" means a device worn by a peace officer that is capable of both video and audio recording of the officer's activities and interactions with others or collecting digital multimedia evidence as part of an investigation;

(2) "portable recording system data" means audio or video data collected by a portable recording system; and

(3) "redact" means to blur video or distort audio so that the identity of the subject in a recording is obscured sufficiently to render the subject unidentifiable.

Sud. 2. Data classification; court-authorized disclosure.

(a) Data collected by a portable recording system are private data on individuals or nonpublic data, subject to the following:

(1) data that document the discharge of a firearm by a peace officer in the course of duty, if a notice is required under section 626.553, subdivision 2, or the use of force by a peace officer that results in substantial bodily harm, as defined in section 609.02, subdivision 7a, are public;

(2) data are public if a subject of the data requests it be made accessible to the public, except that, if practicable, (i) data on a subject who is not a peace officer and who does not consent to the release must be redacted, and (ii) data on a peace officer whose identity is protected under section 13.82, subdivision 17, clause (a), must be redacted;

(3) portable recording system data that are active criminal investigative data are governed by section 13.82, subdivision 7, and portable recording system data that are inactive criminal investigative data are governed by this section;

(4) portable recording system data that are public personnel data under section 13.43, subdivision 2, clause (5), are public; and

(5) data that are not public data under other provisions of this chapter retain that classification.

(b) A law enforcement agency may redact or withhold access to portions of data that are public under this subdivision if those portions of data are clearly offensive to common sensibilities.

(c) Section 13.04, subdivision 2, does not apply to collection of data classified by this subdivision.

(d) Any person may bring an action in the district court located in the county where portable recording system data are being maintained to authorize disclosure of data that are private or nonpublic under

this section or to challenge a determination under paragraph (b) to redact or withhold access to portions of data because the data are clearly offensive to common sensibilities. The person bringing the action must give notice of the action to the law enforcement agency and subjects of the data, if known. The law enforcement agency must give notice to other subjects of the data, if known, who did not receive the notice from the person bringing the action. The court may order that all or part of the data be released to the public or to the person bringing the action. In making this determination, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, to the law enforcement agency, or to a subject of the data and, if the action is challenging a determination under paragraph (b), whether the data are clearly offensive to common sensibilities. The data in dispute must be examined by the court in camera. This paragraph does not affect the right of a defendant in a criminal proceeding to obtain access to portable recording system data under the Rules of Criminal Procedure.

Subd. 3. Retention of data.

(a) Portable recording system data that are not active or inactive criminal investigative data and are not described in paragraph (b) must be maintained for at least 90 days and destroyed according to the agency's records retention schedule approved pursuant to section 138.17.

(b) Portable recording system data must be maintained for at least one year and destroyed according to the agency's records retention schedule approved pursuant to section 138.17 if:

(1) the data document (i) the discharge of a firearm by a peace officer in the course of duty if a notice is required under section 626.553, subdivision 2, or (ii) the use of force by a peace officer that results in substantial bodily harm; or

(2) a formal complaint is made against a peace officer related to the incident.

(c) If a subject of the data submits a written request to the law enforcement agency to retain the recording beyond the applicable retention period for possible evidentiary or exculpatory use related to the circumstances under which the data were collected, the law enforcement agency shall retain the recording for an additional time period requested by the subject of up to 180 days and notify the requester that the recording will then be destroyed unless a new request is made under this paragraph.

(d) Notwithstanding paragraph (b) or (c), a government entity may retain a recording for as long as reasonably necessary for possible evidentiary or exculpatory use related to the incident with respect to which the data were collected.

Subd. 4. Access by data subjects.

(a) For purposes of this chapter, a portable recording system data subject includes the peace officer who collected the data, and any other individual or entity, including any other peace officer, regardless of whether the officer is or can be identified by the recording, whose image or voice is documented in the data.

(b) An individual who is the subject of portable recording system data has access to the data, including data on other individuals who are the subject of the recording. If the individual requests a copy of the

recording, data on other individuals who do not consent to its release must be redacted from the copy. The identity and activities of an on-duty peace officer engaged in an investigation or response to an emergency, incident, or request for service may not be redacted, unless the officer's identity is subject to protection under section 13.82, subdivision 17, clause (a).

Subd. 5. Inventory of portable recording system technology.

A law enforcement agency that uses a portable recording system must maintain the following information, which is public data:

(1) the total number of recording devices owned or maintained by the agency;

(2) a daily record of the total number of recording devices actually deployed and used by officers and, if applicable, the precincts in which they were used;

(3) the policies and procedures for use of portable recording systems required by section 626.8473; and

(4) the total amount of recorded audio and video data collected by the portable recording system and maintained by the agency, the agency's retention schedule for the data, and the agency's procedures for destruction of the data.

Subd. 6. Use of agency-issued portable recording systems.

While on duty, a peace officer may only use a portable recording system issued and maintained by the officer's agency in documenting the officer's activities.

Subd. 7. Authorization to access data.

(a) A law enforcement agency must comply with sections 13.05, subdivision 5, and 13.055 in the operation of portable recording systems and in maintaining portable recording system data.

(b) The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the portable recording system data that are not public only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to the data for a legitimate, specified law enforcement purpose.

Subd. 8. Sharing among agencies.

(a) Portable recording system data that are not public may only be shared with or disseminated to another law enforcement agency, a government entity, or a federal agency upon meeting the standards for requesting access to data as provided in subdivision 7.

(b) If data collected by a portable recording system are shared with another state or local law enforcement agency under this subdivision, the agency that receives the data must comply with all data classification, destruction, and security requirements of this section.

(c) Portable recording system data may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this section or other applicable law.

Subd. 9. Biennial audit.

(a) A law enforcement agency must maintain records showing the date and time portable recording system data were collected and the applicable classification of the data. The law enforcement agency shall arrange for an independent, biennial audit of the data to determine whether data are appropriately classified according to this section, how the data are used, and whether the data are destroyed as required under this section, and to verify compliance with subdivisions 7 and 8. If the governing body with jurisdiction over the budget of the agency determines that the agency is not complying with this section or other applicable law, the governing body may order additional independent audits. Data in the records required under this paragraph are classified as provided in subdivision 2.

(b) The results of the audit are public, except for data that are otherwise classified under law. The governing body with jurisdiction over the budget of the law enforcement agency shall review the results of the audit. If the governing body determines that there is a pattern of substantial noncompliance with this section, the governing body must order that operation of all portable recording systems be suspended until the governing body has authorized the agency to reinstate their use. An order of suspension under this paragraph may only be made following review of the results of the audit and review of the applicable provisions of this chapter, and after providing the agency and members of the public a reasonable opportunity to respond to the audit's findings in a public meeting.

(c) A report summarizing the results of each audit must be provided to the governing body with jurisdiction over the budget of the law enforcement agency and to the Legislative Commission on Data Practices and Personal Data Privacy no later than 60 days following completion of the audit.

Subd. 10. Notification to BCA.

Within ten days of obtaining new surveillance technology that expands the type or scope of surveillance capability of a portable recording system device beyond video or audio recording, a law enforcement agency must notify the Bureau of Criminal Apprehension that it has obtained the new surveillance technology. The notice must include a description of the technology and its surveillance capability and intended uses. The notices are accessible to the public and must be available on the bureau's Web site.

Subd. 11. Portable recording system vendor.

(a) For purposes of this subdivision, "portable recording system vendor" means a person who is not a government entity and who provides services for the creation, collection, retention, maintenance, processing, or dissemination of portable recording system data for a law enforcement agency or other government entity. By providing these services to a government entity, a vendor is subject to all of the requirements of this chapter as if it were a government entity.

(b) A portable recording system vendor that stores portable recording system data in the cloud must protect the data in accordance with the security requirements of the United States Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy 5.4 or its successor version.

(c) Subject to paragraph (d), in an action against a vendor under section 13.08 for a violation of this chapter, the vendor is liable for presumed damages of $2,500 or actual damages, whichever is greater, and reasonable attorney fees.

(d) In an action against a vendor that improperly discloses data made not public by this chapter or any other statute classifying data as not public, the vendor is liable for presumed damages of $10,000 or actual damages, whichever is greater, and reasonable attorney fees.

Subd. 12. Penalties for violation.

In addition to any other remedies provided by law, in the case of a willful violation of this section a law enforcement agency is subject to exemplary damages of not less than twice the minimum, nor more than twice the maximum allowable for exemplary damages under section 13.08, subdivision 1.

13.08 CIVIL REMEDIES.

Subdivision 1.Action for damages.

Notwithstanding section 466.03, a responsible authority or government entity which violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damage as a result of the violation, and the person damaged or a representative in the case of private data on decedents or confidential data on decedents may bring an action against the responsible authority or government entity to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the government entity shall, in addition, be liable to exemplary damages of not less than $1,000, nor more than $15,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under this chapter.

13.09 PENALTIES.

(a) Any person who willfully violates the provisions of this chapter or any rules adopted under this chapter or whose conduct constitutes the knowing unauthorized acquisition of not public data, as defined in section 13.055, subdivision 1, is guilty of a misdemeanor.

(b) Willful violation of this chapter, including any action subject to a criminal penalty under paragraph (a), by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.

Appendix E

Retention of Data

Classification	Definition	Retention
AOA	Footage captured while assisting other agency that may contain evidence	90 days
Arrest	Custodial Arrest	2 years
DWI	Arrest for DWI related offense	2 years
Emer. Veh. Response	Response to CFS that does not result in any other classification	30 days
Flee	Footage of vehicle refusing to stop	2 years
Interview	Interview captured on DVR that does not result in any classification	90 days
Investigative	Community contact of interest; ID poss. suspect; comments required	90 days
Narcotics	Arrest for a narcotics violation	2 years
Test / Accidental Act.	System check at beginning of duty tour / Accidental activation	30 days
Traffic Citation	Traffic Stop resulting in citation issued	180 days
Traffic No Citation	Traffic stop resulting in no citation issued	30 days
Training	Event that could assist in dept. trng - viewable to all personnel	90 days

Appendix E depicts a non inclusive list of retention periods that are reflective of the requirements found in chapter 13.