4-508 BWC and ICC Data Management
(xx/xx/xx)

I. Purpose

Minneapolis Police Department (MPD) members are required to use body worn cameras (BWCs) and in-car cameras (ICCs) in accordance with P&P 4-223. The purpose of this policy is to describe the proper data access, retention, storage, and retrieval processes of data captured by BWCs and ICCs.

II. Procedures/Regulations

A. Data Retention

1. Data will be maintained in a storage system designated and approved by the Department.

   a. All data will be backed up by the storage system vendor.

   b. BWC and ICC video shall only be stored in a database that is CJIS compliant (such as evidence.com, One Drive and Share Point). The video shall not be stored in any other database, including network drives such as the M drive, or on computer hard drives.

2. Data will be retained in accordance with applicable law, this policy, the BWC and ICC Classification Options and Category Guidelines appendix, and the City of Minneapolis' Records Retention Schedules. Data may be retained past the scheduled retention period as required by MN Statute section 13.825 Subd. 2 and Subd. 3.

B. Access to Data and Requests for Duplication of Recordings

1. Permission required for system access

   Access to the Department authorized storage system shall only be granted with written permission from the Commander of the Administrative Services Division (who oversees the Business Technology Unit (BTU)), and only for a legitimate, specified law enforcement purpose.

   a. Such permission must include the level of access to be granted to the person, and any other restrictions to be placed on the access.

   b. BTU will periodically review the user access list to ensure that access levels are appropriate and have been duly authorized, and remove or restrict users as necessary.

2. Documentation of access data

   All accesses of the data are documented automatically as part of the vendor technology. Data relating to accesses will be retained in accordance with the retention schedule for the data that was accessed (see section [II-A]).

3. Requests for data

   All BWC and ICC recordings are the property of the MPD and original recordings shall remain in the sole custody of the MPD, unless necessary for the preparation of civil, criminal or administrative matters, used in court as evidence, provided to an expert for analysis, provided to another law enforcement agency in the scope of their investigation, if required to be provided by lawful order or as otherwise required by the Minnesota Government Data Practices Act or other applicable law.

   a. MPD records policy

      All recordings shall be handled in accordance with P&P 4-501.

   b. Public requests and redaction

      Public requests for BWC or ICC recordings shall be referred to the Records Information unit and will be considered in accordance with the Minnesota Government Data Practices Act or other applicable law.

      i. The public, private, or confidential status will be determined in relation to the specific request.

      ii. All entities with access to BWC or ICC data are responsible for ensuring they only handle and release the data in accordance with MN Statute.

      iii. Any necessary and lawful redaction or other editing of the recordings shall only be completed by Authorized BWC Data Managers in accordance with their lawful duties, records retention laws and policies, and this policy.

         aa. Data that are public may be redacted or access may be withheld to portions of the data if those portions of data are clearly offensive to common sensibilities, in accordance with MN Statute section 13.82 Subd. 7.

         ab. If a data subject requests that data or requests that it be made public, data on other subjects will be redacted as required by MN Statute section 13.825, where applicable.

         ac. The original recording shall remain intact and stored within the Department authorized storage system in accordance with record retention laws and policies.

c. Member requests for duplication

Requests by members for duplication of BWC or ICC data for purposes of official MPD business shall be directed to the Records Information unit.

d. Outside agency requests for duplication

Requests by outside agencies for duplication of BWC or ICC data shall be directed to the Records Information unit.

e. Sharing recordings with the public or with other members

Members shall not share BWC or ICC recordings with any member of the public or any other MPD member, unless it is required in the performance of their official duties and consistent with State and Federal law.

f. Sharing with partner agencies

i. BWC and ICC data may be shared only in the following circumstances:

- With the prosecuting authority for a case.
- With the Office of Police Conduct Review (OPCR) when required for official purposes.
- With the City Auditor when required for official purposes.
- As required by law or court order or for legally required oversight purposes.
- With another law enforcement agency for an active criminal investigation.

ii. If BWC data is shared with another entity, the entity that receives the data must comply with all data classification, destruction, and security requirements of MN Statute section 13.825.

4. Data use for training purposes

Recorded data may only be presented for training purposes with the approval of the Deputy Chief of the Professional Standards Bureau. Nothing herein prohibits Training Division staff from having access to recordings for the purpose of planning training.

5. Data access by members or as evidence

Data captured by a BWC or ICC may be accessed by a member, provided the access is in the course and scope of the member's lawful job duties, such as in the following situations:

- Pending administrative, criminal, civil or traffic matters.
- When investigating a complaint of alleged misconduct.

- In situations where evidence of member misconduct is discovered during the course of authorized access (including force reviews).
- A random or uniform review of the data with regard to equipment functionality or policy compliance.
- Any other purpose authorized under this policy and consistent with State and Federal law.

6. Data access and release in critical incidents

   In any critical incident, video and audio data shall not be accessed unless approved by the investigating agency, except when necessary to comply with the following requirements for release of BWC data in fatal uses of force:

   a. Inspection of BWC data by next of kin within five days

      In accordance with MN Statute section 13.825 Subd. 2(b), where applicable:

      Notwithstanding MN Statute section 13.82 Subd. 7, if a person dies as a result of a use of force by an MPD member, the MPD must allow the following people, upon their request, to inspect all BWC data, redacted no more than what is required by law, documenting the incident within five days of the request, subject to following listed exception:

      i. Specified people

         The people covered by the next of kin inspection requirement are:

         aa. The deceased person's next of kin.

         ab. The legal representative of the deceased person's next of kin.

         ac. The other parent of the deceased person's child.

         "Next of kin" means the surviving spouse or any child of a decedent, or, if there is no surviving spouse or child, the parents of a decedent.

      ii. Exception

         In accordance with MN Statute section 13.825 Subd. 2(c), the MPD may deny a request to inspect BWC data by the specified people in a fatal use of force, if the MPD determines that there is a compelling reason that inspection would interfere with an active investigation. If the MPD denies access under this paragraph, the Chief must provide a prompt, written denial to the specified person who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to MN Statute section 13.82 Subd. 7.

b. Release of BWC data to the public within fourteen days

In accordance with MN Statute section 13.825 Subd. 2(d), where applicable:

If a person dies as a result of a use of force by an MPD member, the MPD shall release all BWC data, redacted no more than what is required by law, documenting the incident no later than 14 days after the incident, unless the Chief asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by MN Statute section 13.82, Subd. 7. This release will be communicated in accordance with the City's Critical Incident Communications Plan.

7. No duplication of data by recording devices

Members are prohibited from using recording devices to duplicate BWC or ICC data in any form, including cell phones or video cameras.

C. Requests for Deletion or Restriction of Accidental or Mistaken Recordings

1. Submitting the request

a. In the event of an accidental or mistaken activation of the BWC where the resulting recording has no investigative or evidentiary value, members may request that their immediate supervisor submit a BWC Accidental Recording Restriction or Deletion Request on their behalf.

i. Deleting footage exposes the MPD to accusations of tampering. Therefore, requests for deletion of BWC footage shall only be made in instances of unintentional BWC activation during non-enforcement or non-investigative activities (e.g., in the restroom or locker room).

ii. If BWC recordings contain evidentiary footage and also contain footage that raises privacy concerns (e.g., undercover officer, filming in a hospital), requests for restriction may be submitted.

iii. Deletion requests of footage that depicts policy violations or misconduct shall not be approved.

b. The supervisor shall complete the request form and indicate if they approve or not.

2. Approved deletion requests

a. Approved deletion requests will be forwarded to BTU. Upon receipt of an approved deletion request, BTU shall review the recording and determine whether or not the recording had an official purpose or evidentiary value.

b. If BTU concurs that the recording has no evidentiary value, BTU shall forward the deletion request to the Commander of Internal Affairs for review.

c. If the Commander of Internal Affairs Division concurs that the recording has no evidentiary value, Internal Affairs shall approve the request and forward it to BTU to delete the recording.

d. A copy of the Body Worn Camera Recording Deletion Request shall be maintained by BTU.

3. Approved restriction requests

a. Approved restriction requests will be forwarded to BTU. If BTU concurs that the recording may be set to restricted access, they will forward the request to the Commander of Internal Affairs for review.

b. If the Commander of Internal Affairs Division concurs with the request, Internal Affairs shall approve the request and forward it to BTU to restrict the recording.

c. BTU shall include the reasons for the restriction in the recording notes within Evidence.com.

D. Notice to Data Subjects

1. If a person brings an action in district court under MN Statute section 13.825 Subd. 2, the MPD shall give notice to any data subjects in the video in question who did not receive notice from the person bringing the action, if known.

2. If the MPD has retained a recording in accordance with MN Statute section 13.825 Subd. 3(d), the MPD shall notify the requester after the time period is up that the recording will then be destroyed unless a new request is made under that paragraph.

3. If the MPD discovers or is notified of a breach in the security of the data, data subjects, if known, will be notified in accordance with MN Statute section 13.055 Subd. 2.