Records Maintenance and Release

804.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of department records. Protected information is separately covered in the Protected Information Policy.

804.1.1 DEFINITIONS

Definitions related to this policy include:

Confidential Data on Individuals - Data classified as confidential by state or federal law and that identifies individuals and cannot be disclosed to the public or even to the individual who is the subject of the data (Minn. Stat. § 13.02, Subd. 3).

Corrections and Detention Data - Data on individuals created, collected, used or maintained because of their lawful confinement or detainment in state reformatories, prisons and correctional facilities, municipal or county jails, lockups, work houses, work farms and all other correctional and detention facilities (Minn. Stat. § 13.85, Subd. 1).

Data on Individuals - All government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual (Minn. Stat. § 13.02, Subd. 5).

Government Data - Data collected, created, received, maintained or disseminated by this department regardless of its physical form, storage media or conditions of use (Minn. Stat. § 13.02, Subd. 7).

Private Data - Data classified as private by state or federal law and that identifies individuals that are only available to the individual who is the subject of the data or with the individual’s consent (Minn. Stat. § 13.02, Subd. 12).

804.2 POLICY

The Columbia Heights Police Department is committed to providing public access to records and data in a manner that is consistent with the Minnesota Government Data Practices Act (MGDPA) and Official Records Act (Minn. Stat. § 13.03; Minn. Stat. § 15.17).

804.3 CUSTODIAN OF RECORDS RESPONSIBILITIES

The Chief of Police shall designate a Custodian of Records. The responsibilities of the Custodian of Records include, but are not limited to:

(a) Managing the records management system for the Department, including the retention, archiving, release, and destruction of department data (Minn. Stat. § 15.17; Minn. Stat. § 138.17, Subd. 7).

(b) Maintaining and updating the department records retention schedule, including:

    1. Identifying the minimum length of time the Department must keep data.

2. Identifying the department division responsible for the original data.

(c) Establishing rules regarding the inspection and copying of department data as reasonably necessary for the protection of such data.

(d) Identifying data or portions of data that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of data.

(f) Ensuring a current schedule of fees for public data as allowed by law is available.

(g) Ensuring the posting or availability to the public a document that contains the basic rights of a person who requests government data, the responsibilities of the Department, and any associated fees (Minn. Stat. § 13.025).

(h) Ensuring data created by the Department is inventoried and subject to inspection and release pursuant to lawful requests consistent with the MGDPA requirements (Minn. Stat. § 13.03, Subd. 1).

(i) Ensuring that the current version of each department policy identified in Minn. R. 6700.1615 is posted on the department's website or otherwise posted in the public area of the Department in accordance with Minn. R. 6700.1615 (Minn. R. 6700.1615, Subd. 2).

804.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any department member who receives a request for data shall route the request to the Custodian of Records or the authorized designee.

804.4.1 REQUESTS FOR RECORDS

The processing of requests for data is subject to the following:

(a) A person shall be permitted to inspect and copy public government data upon request at reasonable times and places and shall be informed of the data's meaning if requested (Minn. Stat. § 13.03, Subd. 3).

1. The Department may not charge or require the requesting person to pay a fee to inspect data. Inspection includes, but is not limited to, the visual inspection of paper and similar types of government data. Inspection does not include printing copies, unless printing a copy is the only method to provide for inspection of the data (Minn. Stat. § 13.03, Subd. 3(b)).

2. For data stored and made available in electronic form via remote access, public inspection includes allowing remote access by the public to the data and the ability to print copies or download the data. A fee may be charged for remote access to data where either the data or the access is enhanced at the request of the person seeking access (Minn. Stat. § 13.03, Subd. 3(b)).

(b) Government data maintained by this department using a computer storage medium shall be provided in that medium in electronic form, if a copy can be reasonably made. The Department is not required to provide the data in an electronic format or program that is different from the format or program in which the data is maintained (Minn. Stat. § 13.03, Subd. 3 (e)).

(c) The Department is not required to create records that do not exist.

(d) The Custodian of Records or designee processing the request shall determine if the requested data is available and, if so, whether the data is restricted from release or denied. The Custodian of Records or designee shall inform the requesting person of the determination either orally at the time of the request or in writing as soon after that time as reasonably possible. The Custodian of Records or designee shall cite the specific statutory section, temporary classification or specific provision of state or federal law on which the determination is based. Upon the request of any person denied access to data, the denial shall be certified in writing (Minn. Stat. § 13.03, Subd. 3 (f)).

(e) When a record contains data with release restrictions and data that is not subject to release restrictions, the restricted data shall be redacted and the unrestricted data released.

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the department-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

804.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Personal identifying information, including an individual’s photograph; Social Security and driver identification numbers; name, address, and telephone number; and medical or disability information that is contained in any driver’s license record, motor vehicle record, or any department record, including traffic collision reports, is restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Private data on the following individuals (Minn. Stat. § 13.82, Subd. 17):

1. An undercover law enforcement officer.

2. A victim or alleged victim of criminal sexual conduct, or sex trafficking, or of a violation of Minn. Stat. § 617.246, Subd. 2.

3. A paid or unpaid informant if the Department reasonably believes revealing the identity would threaten the personal safety of the informant.

4. A victim of or witness to a crime if the victim or witness specifically requests not to be identified publicly, unless the Department reasonably determines that revealing the identity of the victim or witness would not threaten the personal safety or property of the individual.

5. A person who placed a call to a 9-1-1 system or the identity of the person whose phone was used to place a call to the 9-1-1 system when revealing the identity may threaten the personal safety or property of any person or the purpose of the call was to receive help in a mental health emergency. A voice recording of a call placed to the 9-1-1 system is deemed to reveal the identity of the caller.

6. A juvenile witness when the subject matter of the investigation justifies protecting the identity of the witness.

7. A mandated reporter.

(c) Audio recordings of calls placed to the 9-1-1 system requesting law enforcement, fire, or medical agency response, except that a written transcript of the call is public unless it reveals the identity of protected individuals (Minn. Stat. § 13.82, Subd. 4).

(d) Criminal investigative data involving active cases and inactive investigative data (Minn. Stat. § 13.82, Subd. 7):

1. If the release of the data would jeopardize another ongoing investigation or would reveal the identity of protected individuals or is otherwise restricted.

2. Images and recordings, including photographs, video, and audio records that are clearly offensive to common sensibilities. However, the existence of any such image or recording shall be disclosed.

3. As otherwise restricted by law.

(e) Juvenile records and data (Minn. Stat. § 260B.171).

(f) State criminal history data held in the Bureau of Criminal Apprehension (BCA) database, including but not limited to fingerprints, photographs, identification data, arrest data, prosecution data, criminal court data, and custody and supervision data (Minn. Stat. § 13.87).

(g) Traffic collision reports and related supplemental information (Minn. Stat. § 169.09, Subd. 13).

(h) Corrections and detention data (Minn. Stat. § 13.85).

(i) Personnel data except, unless otherwise restricted (Minn. Stat. § 13.43, Subd. 2):

1. Name, employee identification number, and some aspects of compensation.

2. Job title, bargaining unit, job description, education and training background, and previous work experience.

3. Date of first and last employment.

4. Existence and status of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action.

5. Final disposition of any disciplinary action together with the specific reasons for the action, and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of this department.

6. Terms of any agreement settling any dispute arising out of an employment relationship.

7. Work location, work telephone number, badge number, and honors and awards received.

8. Time sheets or other comparable data only used to account for an employee's work time for payroll purposes, excluding the use of sick or other medical leave or other nonpublic data.

9. All other personnel data regarding employees of this department are private data and may only be released as authorized by that classification.

(j) Any data that was created under the direction or authority of the City Attorney exclusively in anticipation of potential litigation involving this department shall be classified as protected nonpublic or confidential data while such action is pending (Minn. Stat. § 13.39).

(k) All data collected by an Automated License Plate Reader (ALPR) on individuals or nonpublic data absent an exception (Minn. Stat. § 13.82; Minn. Stat. § 13.824).

(l) Response or incident data, so long as the Custodian of Records determines that public access would likely endanger the physical safety of an individual or cause a perpetrator to flee, evade detection, or destroy evidence (Minn. Stat. § 13.82, Subd. 14).

(m) Any data on individuals receiving peer counseling or critical incident stress management services (Minn. Stat. § 13.02, Subd. 12; Minn. Stat. § 181.9731; Minn. Stat. § 181.9732).

Any other record not addressed in this policy shall not be subject to release where such record is classified as other than public data. All public data shall be released as required by the MGDPA (Minn. Stat. § 13.03, Subd. 1).

804.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for data should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested data.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the Prosecuting Attorney, City Attorney or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

804.7 RELEASED RECORDS TO BE MARKED

Each audio/video recording released shall include the department name and to whom the record was released.

804.8 EXPUNGEMENT

A petition for expungement and expungement orders received by the Department shall be reviewed for appropriate action by the Custodian of Records.

804.8.1 PETITION FOR EXPUNGEMENT

When responding to a petition for expungement, the Custodian of Records shall inform the court and the individual seeking expungement that the response contains private or confidential data (Minn. Stat. § 609A.03, Subd. 3).

804.8.2 ORDERS OF EXPUNGEMENT

The Custodian of Records shall expunge such records as ordered by the court. Records may include, but are not limited to, a record of arrest, investigation, detention or conviction. Once a record is expunged, members shall respond to any inquiry as though the record did not exist.

Upon request by the individual whose records are to be expunged, the Custodian of Records must send a letter at an address provided by the individual confirming the receipt of the expungement order and that the record has been expunged (Minn. Stat. § 609A.03, Subd. 8).

Expunged records may be opened only by court order (Minn. Stat. § 609A.03, Subd. 7).

Expunged records of conviction may be opened for purposes of evaluating a prospective employee of the Department without a court order.

The Custodian of Records shall inform any law enforcement, prosecution or corrections authority, upon request, of the existence of a sealed record and of the right to obtain access to it.

804.9 MAINTENANCE OF CLOSED RECORDS

Records such as offense reports, arrest reports, juvenile records or other sensitive records shall be secured in such a manner as to reasonably protect them from unauthorized disclosure. Closed records shall be kept separate from public records and shall remain confidential.

804.10 DATA PRACTICES PLAN

See attachment: CHPD Data Practices Plan 12-2022.pdf

Attachments

CHPD Data Practices Plan 12-2022.pdf

Columbia Heights Police Department

Data Practices Plan

Effective date: December 1, 2011

Reviewed: December 12, 2012
Reviewed: December 04, 2013
Reviewed: December 12, 2014
Reviewed: December 28, 2015
Reviewed: December 20, 2016 (amended/includes Body Worn Camera data)
Reviewed: December 28, 2017
Reviewed: December 03, 2018
Reviewed: December 17, 2019 (amended/includes retention schedule)
Reviewed: December 08, 2020
Reviewed: December 08, 2021
Reviewed: December 06, 2022 (amended to align with Lexipol policy 804)

DATA PRACTICES PLAN

I. PURPOSE

The purpose of this Data Practices Plan is to develop policy and procedure as required by Minnesota State Statute, Chapter 13, Minnesota Government Data Practices Act, and Chapter 1205, the Department of Administration, Data Privacy Division, Data Practices rules. It is the intent of the Columbia Heights Police Department to comply with all laws and rules regarding government data and conduct its operation efficiently and effectively regarding the data it collects, stores and disseminates. The "Data Practices Plan" will be kept by the Police Office Supervisor and be available for review upon request.

II. RESPONSIBLE AUTHORITY

A. The Responsible Authority for the City of Columbia Heights is the City Manager. The City Manager has delegated this position regarding Police Department data to the Chief of Police. The Chief of Police, by virtue of inclusion in the job description, has delegated the Custodian of Records position to the Police Office Supervisor.

B. The Police Office Supervisor assumes the following Custodian of Records duties:

   a. Managing the records management system for the Department, including the retention, archiving, release, and destruction of department data (Minn. Stat. § 15.17; Minn. Stat. § 138.17, Subd. 7).
   b. Maintaining and updating the department records retention schedule, including:
      1. Identifying the minimum length of time the Department must keep data.
      2. Identifying the department division responsible for the original data.
   c. Establishing rules regarding the inspection and copying of department data as reasonably necessary for the protection of such data.
   d. Identifying data or portions of data that are confidential under state or federal law and not open for inspection or copying.
   e. Establishing rules regarding the processing of subpoenas for the production of data.
   f. Ensuring a current schedule of fees for public data as allowed by law is available.
   g. Ensuring the posting or availability to the public a document that contains the basic rights of a person who requests government data, the responsibilities of the Department, and any associated fees (Minn. Stat. § 13.025).
   h. Ensuring data created by the Department is inventoried and subject to inspection and release pursuant to lawful requests consistent with the MGDPA requirements (Minn. Stat. § 13.03, Subd. 1).

III. ACCESS TO PUBLIC DATA

A. *Public* data is all data collected, created, received, maintained or disseminated by the Columbia Heights Police Department which is not classified by statute, temporary classification pursuant to section 13.06, or federal law, as *non-public* or *protected non-public*, or with respect to data on individuals, as *private* or *confidential*.

B. *Public* data can be accessed by presenting an in-person request at the Police Department window at the Public Safety Building, 825 41st Avenue NE, Columbia Heights, MN 55421, during normal business hours.

1. Normal business hours are 8:00 a.m. to 4:30 p.m. daily excluding weekends and legal holidays.

2. Requests for *public* data will also be accepted in writing via letter, fax or email at any time. Such requests will be processed during normal business hours.

C. Requests for *public* data will be processed and eligible data provided as soon as possible upon receipt and processing of the request. A reasonable response time will be maintained with the amount of time governed by issues such as:

1. Determination by the Custodian of Records (in some cases) of the classification of the data requested;

2. Redaction or summarization of the data as may be required;

3. Location (off-site, on-site) or storage medium (electronic, paper) of the data requested.

D. Police reports (otherwise known as ICR's or Initial Contact Reports) may not be available for three to five business days since the date of the incident. This is to allow for report processing.

E. A Data Request Form shall be filed in the Completed Request for Information folder.

IV. ACCESS TO PRIVATE DATA

A. *Private* data is data on individuals which is made by statute or federal law not *public* and accessible to the individual subject of that data.

B. Requests for access to *private* data must be forwarded to the Police Office Supervisor. Only the Police Office Supervisor may officially receive and approve/disapprove requests to access *private* data.

1. If the Police Office Supervisor is to be absent for an extended period

of time (over five business days), the responsibilities are to be delegated to Lead Record Tech or Captain.

C. The following shall have access to *private* data:

1. The subject(s) of the data;

2. City of Columbia Heights and Columbia Heights Police Department employees whose work assignments require access;

3. Other governmental agencies and entities that are authorized by state statute or federal law to access *private* data;

4. Attorneys, legal representatives and agents of the City of Columbia Heights and Columbia Heights Police Department who have a documented need in response to a current or pending legal action (either civil or criminal);

5. Individuals or entities given specific written and signed authority by the subject(s) of the *private* data.

D. Requests for *private* data:

1. Requests for *private* data will be received and processed during normal business hours as defined in III, Paragraph B, Section 1.

2. In-person requests by the data subject(s) require a confirmation of their identities prior to access to said data. Confirmation can be in the form of:

   a) Drivers license or state identification card;

   b) Picture identification from a known institution;

   c) Verification of identity by a reliable third party.

3. Written requests, for *private* data by the data subject(s) must bear original signatures; and if submitted by mail, must be notarized.

4. Written authorizations for third party access to *private* data must bear the original signature(s) of the subject(s) and must be either notarized or witnessed. The third party being given authorization to the *private* data must be specifically identified. The *private* data which authority to access is being given must be specifically identified. Persons presenting authorization forms from data subjects are to be identified as specified in IV, Paragraph D, Section 2.

G. A Request for Information will be filled out when *private* data is accessed by the subject(s) or their authorized agents. The written request will be filed in the Completed Request for Information folder.

H. Upon receipt by the Police Office Supervisor (or delegate), requests for *private* data will be processed immediately. If circumstances do not allow for immediate processing or access to the data by the subject, access will be given within ten business days.

I. Requests for access to *private* data which are denied will be given the reason(s) orally at the time of the request and the statutory or federal law basis for this decision.

1. The person being denied access can request a written justification for the denial. The Police Office Supervisor (or designee) will then provide, in writing, that the request was denied and the statutory basis or federal law the denial was based upon.

J. The Peace Officer Discipline and Procedures Act, Minnesota Statute 626.89, Subdivision 5, requires that a peace officer be provided a signed written complaint and a summary of allegations prior to the taking of any formal statement from said officer. This complaint and summary may contain *private* data and therefore must be maintained and disseminated in accordance with applicable Minnesota state law and this plan.

V. ACCESS TO CONFIDENTIAL DATA:

A. *Confidential* data is data on individuals which is made *not public* by statute or federal law applicable to the data, and is inaccessible to the individual subject of that data.

B. The following may have access to *confidential* data:

1. City of Columbia Heights and Columbia Heights Police Department employees or agents whose work assignment or responsibilities reasonably require access;

2. Entities and agencies authorized by Minnesota state statutes or federal law to access that specific data.

C. Access to *confidential* data:

1. Requests to access *confidential* data will be received as detailed in III, Paragraph B, Section 1 of this plan;

2. Requests to access *confidential* data will be processed as detailed in IV, Paragraph D, Sections 1, 2, 3 and 4 of this plan;

3. *Confidential* data shall not be disclosed to the subject of said data or,

to anyone else not authorized by Minnesota state statutes or federal law;

4. The subject of *confidential* data will be informed upon receipt of their written request whether or not *confidential* data is retained on them. A copy of this request will be attached to the *confidential* data.

D. The Peace Officer Discipline and Procedures Act, Minnesota Statute 626.89, Subdivision 5, requires that a peace officer be provided a signed written complaint and a summary of allegations prior to the taking of any formal statement from said officer. This complaint and summary may contain "Confidential" data and therefore must be maintained and disseminated in accordance with applicable Minnesota state law and this plan.

VI. ACCESS TO JUVENILE DATA

A. The Columbia Heights Police Department only maintains peace officer records of juveniles as defined Chapter 260B of Minnesota state law.

B. Access to peace officer's records concerning juveniles is governed by Minnesota Statute 260B.171, Subdivision 5.

1. Access to juvenile records may be made as follows:

a) By order of the juvenile court;

b) As required by M.S.S. 121A.286 (drug incident data to the juvenile's school);

c) As authorized under M.S.S. 13.82, subdivision 2 (arrest data minus name, age and address);

d) To the juvenile or the juvenile's parent or guardian unless disclosure of the record would interfere with an ongoing investigation; or,

e) Traffic accident reports which include juvenile names may be accessed and released, except that names of juveniles charged or cited with law or ordinance violations related to the accident must be removed or redacted.

2. It is a misdemeanor offense to release or discuss the contents of juvenile record other than as provided by Minnesota State Statutes.

C. Requests to access juvenile records:

1. Requests to access juvenile case records other than as authorized by VI, Paragraph B, Section 1 shall be denied by receiving departmental

personnel;

2. Requesters shall be informed of the reason for the denial and the statutory basis;

3. Requesters will be provided with the juvenile's initials, and the address and phone number of the Anoka County Juvenile Court so they can forward their request appropriately.

D. The Police Office Supervisor will receive any standing orders from the juvenile court or county attorney regarding releasing of juvenile data. Said orders will be maintained in the Data Practices Plan and disseminated to appropriate departmental staff.

E. Copies of Juvenile Court Orders releasing data will be attached to the originals of all such data released.

VII. ACCESS TO SUMMARY DATA

A. *Summary* data are statistical records and reports derived from data on individuals, but in which individuals are not identified, and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

B. Persons wishing access to *summary* data must submit a written request to the Police Office Supervisor. This written request must contain the following:

1. The precise nature and detail of the data desired;

2. The date(s) or date range(s) to be searched;

3. The purpose for which the *summary* data is being requested;

4. Willingness to pay, either in advance or upon receipt, any reasonable cost and fees incurred to prepare and copy the *summary* data;

5. Written request is signed and dated by the requester.

C. Procedures to access *summary* data:

1. Requests for *summary* data will only be received by the Police Office Supervisor (or delegate) during "normal business hours" as defined in III, Paragraph B;

2. Requests received will be checked for compliance with VII, Paragraph B, Sections 1 through 6. Requests missing information will be returned to the requester noting what additions or changes are necessary;

3. Appropriate requests will be processed by the Police Office Supervisor (or delegate) with an acknowledgment sent to the requester. This will be done within 10 working days of receipt of the request. This letter may contain any of the following:

   a) Estimated cost of providing the *summary* data requested;

   b) The *summary* data requested;

   c) The time schedule in which the *summary* data will be provided and the reason(s) if the time to respond is over 15 working days;

   d) A schedule of dates and times the requester may come to the Columbia Heights Police Facility to access *private* and *confidential* data so they can prepare the *summary* data themselves, or;

   e) The reason(s) why the request for *summary* data is being denied.

   f) Names and other unique personal identifiers are to be redacted when preparing *summary* data.

VIII. RIGHTS OF SUBJECTS OF DATA

A. Individuals have the right to access data. Their request must be presented to the Police Office Supervisor (or delegate). Access to *public* dated is outlined in III of this plan, access to *private* data is outlined in IV of this plan, and access to *confidential* data is outlined in V of this plan.

B. Individual subjects of data may contest the accuracy or completeness of *public* or *private* data on themselves. To do so, said individual shall notify the Police Office Supervisor describing the nature of the disagreement. The Police Office Supervisor (or delegate) must within 30 days:

   1. Correct the data found to be inaccurate or incomplete and attempt to notify past recipients of said data including those identified by the individual as recipients, or;

   2. Notify the individual that the data is believed to be correct or complete.

C. Written challenges to the accuracy or completeness of *public* or *private* data shall be attached to said data and released along with the data when accessed.

D. Decisions regarding the accuracy and completeness of *public* and *private* data may be appealed by the subject to the Commissioner of Administration. Data successfully challenged by an individual must be completed, corrected or destroyed by the Director of Services (or delegate) and a copy of the Commissioner's Order attached to said data.

IX. FEE STRUCTURE

A. *Public* and *private* data may be accessed and viewed at the Columbia Heights Police Facility for no charge. Additionally, no fee may be assessed for separating *public* from not *public* data when it is only viewed.

B. Copies and electronic transmittals of *public* and *private* data will be assessed a fee commensurate with the costs of making, certifying, compiling and mailing the records. This will include the cost of employee time.

C. Copies of *public* data that has commercial value may be assessed an additional fee along with that listed in IX, Paragraph B, as may be determined and appropriately justified by the Police Office Supervisor.

D. Copies of data provided to agencies of government (other than City of Columbia Heights) may be charged the same as individuals.

E. All reasonable costs in preparing *summary* data shall be paid by the requester, either in advance or upon receipt of the data. A breakdown of these costs will be provided by the Police Office Supervisor (or delegate).

F. Fee schedules related to data requests and copies will be prepared by the Police Office Supervisor and given to the Columbia Heights City Council for adoption into the City's fee schedule.

G. Waiver of fees is the sole authority of the Columbia Heights City Council or the Responsible Authority for the City. Persons wishing a fee waiver must seek prior City Council approval or the City's Responsible Authority.

X. PENALTY PROVISIONS

A. Minnesota Statute Section 13.09 states, "Any person who willfully violates provisions of this chapter (Government Data Practices Act) is guilty of a misdemeanor. Willful violation of the chapter by any public employee constitutes just cause for suspension without pay or dismissal of the public employee."

B. Departmental staff must pay special attention to the provisions contained in CHPD Policy 804 and Minnesota Statute 13, "Government Data Practices Act". Violations of either Policy 804 or Minnesota Statute 13 may result in disciplinary action in accordance with Departmental Rules and Regulations.

XI. ACCESS TO BODY WORN CAMERA DATA

A. Duplication of Tapes/Media

The original media is to remain in the custody of the Columbia Heights Police Department at all times.

B. Requests for Media
Requests for duplication of recorded media from public or private concerns shall be provided in accordance with the data practices policy outlined in Policy 804, Records Maintenance and Release. The requestor must pay the fee for duplicating the media prior to the copy being made.

Certain file management software, including evidence.com managed by Taser Inc., has the capability to share media files electronically. Only Columbia Heights officers authorized to do so, may electronically share media files with other law enforcement agencies, or county departments, as part of an active or potential investigation. Any other request should follow the normal procedure for release of information.

C. Data Subjects: Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

1. Any person or entity whose image or voice is documented in the data (M.S. 13.825, subd. 4(a)).
2. The Officer who collected the data (M.S. 13.825, subd. 4(a))
3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording. (M.S. 13.825, subd. 4(a)).

Privacy: BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

BWC data pertaining to people is presumed private, as is BWC pertaining to businesses or other entities (M.S. 13.825, subd. 2(a). However, some BWC data is classified as confidential, and some BWC data is classified as public:

D. Confidential Data:
BWC data that is collected or created as part of an active criminal investigation is confidential while the investigation remains active. (M.S. 13.82, subd. 7.). This classification takes precedence over the "private classification listed above and the "public" data classification listed below. (M.S. 13.825, subd. (2)(a)(3).

E. Public Data: The following BWC data is public:
1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous. (M.S. 13.82, subd. 2(a)(1).
2. Data that documents the use of force by a peace officer that results in substantial bodily harm. (M.S. 13.82, subd. 2(a.)(1).
3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted. In addition, any data

on undercover officers must also be redacted. (M.S. 13.825, subd. 2; M.S. 13.82, subd. 17(a).

4. Data that documents the final disposition of a disciplinary action against a public employee. (M.S. 13.825, subd._2(a)(4);M.S. 13.43, subd. 2(5).

However, if another provision of the Data Practices Act classifies data as private or otherwise public, the data retains that other classification. (M.S. 13.825, subd. 2(a)(5). For instance, data that reveals protected identities under M.S. 13.82, subd. 17 should not be released even if it would otherwise fit into one of the public categories listed above.

F. Records to Maintain:
The department will maintain the following records and documents relating to BWC use, which are classified as public data (M.S. 13.825, subd. 5):

1. The total number of BWCs owned by the agency;
2. A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;
3. The total amount of recorded BWC data collected and maintained; and
4. This policy, together with the Records Retention Schedule.

G. Access to BWC data by non-employees:
Officers shall refer members of the media or public seeking access to BWC data to the department Office Supervisor, who shall process the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded BWC data about that person and other data subjects in the recording (M.S. 13.825, subd. 4(b)), except when:
    a. The data was collected or created, and is being maintained as part of an ongoing investigation (M.S. 13.82, subd. 7; and
    b. Access shall not be granted to portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as the identities of informants, certain witnesses, juvenile offenders, and victims of criminal sexual conduct or sex trafficking. (M.S. 13.82, subd. 17).
2. An individual data subject shall be provided with a copy of the recording upon request but subject to the following guidelines on redaction before the copy is provided (M.S. 13.825, subd. 4(b)):
3. Data on other individuals in the recording who do not consent to the release must be redacted.
4. Data that would identify undercover officers must be redacted. Data on other Officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

H. Access by Police Officers and Law Enforcement Employees:

No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes. In addition, Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.

Agency personnel shall document their reason for accessing stored BWC data at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.

Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

I. Other Authorized Disclosures of Data:
Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. 13.82 subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying the video. In addition:

1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes and are documented in writing at the time of the disclosure.
2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

Lenny Austin
Chief of Police

Karen Olson

Karen Olson
Police Office Supervisor

Electronic File Retention (BWC)

Uncategorized:	1 year
Death Investigation:	Until manually deleted
Drug Task Force:	7 years
Garbage/DEMO:	90 days
Misc. Report/CFS/ Warrant Arrest, etc:	1 year
Officer Injury:	Until manually deleted
P.C. Arrest:	7 years
Pending Review:	Until manually deleted
Photos & Audio Statements:	10 years
Restricted:	Until manually deleted
Traffic Citation:	1 year
Traffic Stop:	1 year
Use of Force:	7 years