235.00 Data Practices

The Minnesota Data Practices Act imposes on an employee a criminal (misdemeanor) and civil penalty (suspension/termination) for willful violations of the law. This penalty may be for either a wrongful dissemination or withholding of information. Every member of the department must be aware of the significance of this Act and the procedures established to assure proper compliance.

All Saint Paul Police Department policies and practices respecting data collection (Minnesota Statute 13.02 Subd. 7) and dissemination are based on the Minnesota Data Practices Act, Minnesota Statute 13.82. Due to the dynamic nature of laws and legislation, this statute is incorporated by reference into this policy manual. It is impractical to attempt to list in this policy all data practices affecting law enforcement. Any questions maybe directed to the department's data compliance officer or records manager. The city attorney is also available to respond to difficult questions regarding data practices.

Government Data:
"Government data" means all data collected, created, received, maintained or disseminated by the department regardless of its physical form, storage media or conditions of use.
It is the policy of this department that all private, confidential or non-public government data, shall be accessed for official purposes only. Internal requests for such information shall be made only by members whose official police business necessitates having access to such information. Under no circumstances will this information be disseminated outside the agency, other than through approved procedures and in accordance with the Minnesota Data Practices Act.

Access Procedures:
Requests for information can typically be classified into two types:
1. Requests from the media.
2. Requests for information from the general public (citizens, victims, witnesses, attorneys, etc.)

Media Requests:
The public information officer (PIO) who works out of the chief's office is the point of first contact for all media requests. In the event that the PIO is unavailable, an inspector or the watch commander may handle the request in accordance with General Order: 235.60 News Media.

General Public:
The general intake point for all requests, except media, will be handled by the records unit. Due to the varied circumstances that can occur concerning dissemination of information, it is the intent of this policy that the data compliance officer and the records manager work closely to ensure an appropriate response to requests within the policies, federal and state laws.

Police Data for Private Use:
- No employee will view or obtain data for private use while on duty. All information obtained while on duty status must be for official departmental use.
- Employees seeking information for private use shall conduct their business at the public counter of the records unit, on their own time, and shall pay all fees, as any other private citizen.
- Obtaining copies of information intended for private use without paying the normal fees constitutes theft.

Confidential Criminal Data:
All criminal data gathered as part of an ongoing investigation is confidential while the investigation is active and/or the case is pending in the court system.

An investigation becomes inactive upon the occurrence of any of the following events:
1. A decision by the department to close the investigation and no longer pursue the case.
2. The statute of limitations has run.
3. The prosecution has declined to prosecute.
4. The case is dismissed, or the defendant is found not guilty in court.
5. Exhaustion of or expiration of all rights of appeal by an individual convicted on the basis of the investigative data.

(See General Order 235.50: Uniform Evidence Retention)

Cases determined to be inactive will become active and confidential upon a departmental determination to reopen the investigation.

The data compliance officer, public information officer and records manager in responding to requests for criminal data, must be able to rely on the present information in the record unit's files. The department policy of all reports being processed, cataloged and stored within the records unit, is essential.

Revised July 1, 2011