CITY OF BLAINE

RECORDS MANAGEMENT/
DATA PRACTICES POLICIES

November 2019

Purpose

The purpose of the City of Blaine's Records Management/Data Practices Policy is twofold: first, it provides a plan for managing government records by allowing continuing authority to dispose of records under Minnesota Statutes section 138.17; and second, it satisfies the requirement in Minnesota Statutes, Section 13.025 government entity obligation, Section 13.03 procedures, and Section 13.05, duties of responsible authority, including the establishment of procedures ensuring appropriate access to not public data.

Questions regarding this document can be addressed to:

CATHERINE M. SORENSEN
CITY CLERK
10801 TOWN SQUARE DRIVE
BLAINE MN 55449
(763) 784-6124
csorensen@blainemn.gov

Questions about Archival Records:
Minnesota Historical Society State Archives Department Minnesota History Center 345 West Kellogg Boulevard
St. Paul, MN 55102-1906
651-259-3260 or 800-657-3773
Email: statearchives@mnhs.org
http://www.mnhs.org/preserve/records/

Questions about Data Practices:
Department of Administration Data Practices Office
320 Centennial Office Building
658 Cedar St.
St. Paul, MN 55155
651-296-6733 or 800-657-3721
Email: info.dpo@state.mn.us
https://mn.gov/admin/data-practices/

Records Management Program History and Purpose

The City of Blaine first adopted a records retention schedule in 1980. In 1984, the schedule was updated and revised, and the city adopted the entire general record retention schedule (GRRS) in August 1989. In 1994 city clerks and officials representing the Minnesota Clerks and Finance Officers Association (MCFOA) and Association of Records Managers and Administrators (ARMA) Twin Cities Chapter updated the GRRS, and as the GRRS is updated, the city will incorporate updates as necessary.

In 1996, the GRRS was revised to reflect the changing requirements of the city by adding new records series and descriptions to help clarify items. During the summer of 1997, the data classification portion of the GRRS was reviewed in more detail and upon review, changes were sent to the State for approval. During 2007, the entire GRRS was reviewed again and in 2017 the city council adopted the latest update produced by the Minnesota Clerks and Finance Officers Association (MCFOA). The City will continue to adopt and follow the most recent General Records Retention Schedule.

SECTION I – RECORDS MANAGEMENT

Retention Schedule

The city council formally adopted the May 2017 update to the general records retention schedule for Minnesota cities on July 13, 2017. The purpose of a records retention schedule is to provide a plan for managing government records by giving continuing authority to dispose of records under Minnesota Statutes section 138.17. The GRRS establishes minimum retention periods for city records based on their administrative, fiscal, legal and historical value. While the city may not necessarily collect all records identified, the GRRS lists record series common to cities and identifies how long to retain them. The document is always evolving therefore the most recent Records Retention Schedule for Minnesota Cities posted by the Minnesota Clerks and Finance Officers Association (MCFOA) will be followed.

Duplicate Records

This retention schedule concerns itself only with the city's official record copy and the retention periods assigned reflect that. It is each city's responsibility to identify the official record copy and to identify when to destroy any other copies of identical records, after they have lost their legal, fiscal, historical and administrative value. Duplicate copies should not be retained as long as the official record. Normally the retention period on duplicate records will not exceed two years.

Maintaining the General Records Retention Schedule

The records management database was designed during the summer of 1996, revised in the summer of 1997 and again in 2007. The city currently follows the most recently adopted General Records Retention Schedule for Minnesota Cities produced by the Minnesota Clerks and Finance Officers Association, which is updated periodically in conjunction with the Minnesota State Department of Administration, Information Policy Analysis Division and the Minnesota Historical Society.

Destruction Eligibility Report

A destruction eligibility report has been created and includes information to make the purging process easier. In January of each year the City Clerk's Office will distribute the most recent GRRS to all departments in order to prepare for destruction of any records which have reached their retention period based on the adopted schedule.

- **Section:** The section of the GRRS where the records are compiled
- **Records Series Code:** The code that relates to the records in the GRRS
- **Record Series Title/Description:** The title of the record and additional description
- **Retention Period:** The length of time the record is to be retained.
- **Data Practices Classification:** The data's classification of public/private/non-public/confidential
- **Data Practices Statute:** Refers to the statute or law which cites the data practices classification of the record series.
- **Destroy Records Created Before This Date:** Indicates that if this type of record was created before this date, destruction can be completed.
- **Condition for the Destruction of the Record:** The exception criteria or instruction to be met prior to destruction.
- **Destruction Method:** (Recycle, Shred, or Permanent, Delete) This indicates how the record should be disposed.

Destruction of Records

The destruction of records should be followed according to the adopted GRRS. In accordance with administrative policy, most of the destruction of records will be completed after January 1 and before February 15 of each year. Occasionally an employee might have a record that has a retention period noted by the number of months. If destruction is completed annually or during other times of the year, the **Records Destruction Report** must be completed and submitted to City Clerk staff at that time. After records are destroyed according to the **Records Retention Schedule** the report will be placed on file.

City Clerk's staff and department staff will also monitor **DocuWare retention** for a list of records for disposal that have been imaged. After purging the items in the listing the City Clerk's staff will then complete the **Records Destruction Report** and place on file in the City Clerk's Office.

Records that are not on the adopted GRRS and determined to be in need of disposal are treated with a different procedure than the destruction procedure previously illustrated. An **Application for Authority to Dispose of Records** needs to be completed with the records description and location. This form will not provide continuous authority to dispose of similar records and cannot be used to approve a GRRS. City Clerk staff will process all disposal requests of this type on behalf of the city with the State Archives Department who will be notified.

Inventory Maintenance

Records inventory will be maintained on a regular basis. Each department will be audited once a year to determine if a new record series has been created and, if so, the new record will be reviewed and included in the GRRS. It is each department's administrative personnel's responsibility to keep the GRRS current with items in the department. The audit will help ensure that each department is complying and City Clerk staff will conduct the audit. All applications for authority to dispose of records shall be completed and filed with the City Clerk's Office. When adding a new item to the Retention Schedule, follow the steps in the Retention Schedule section of this manual. The department should follow this process for the annual records audit.

SECTION II – DATA CLASSIFICATION

These procedures have been implemented to comply with the requirements of the Minnesota Data Practices Act, specifically Minnesota Statutes Sections 13.025, 13.03, Subd. 2 and 13.05, Subd. 5.

The Government Data Practices Act (Minnesota Statutes, Chapter 13) presumes that all government data are public unless a state or federal law says the data are not public. Government data means all recorded information a government entity has, including paper, email, flash drives, CDs, DVDs, photographs, etc.

The law also says that the city must keep all government data in a way that makes it easy to access public data. A requestor has the right to look at (inspect), free of charge, all public data kept and also has the right to obtain copies of public data. The Data Practices Act allows a city to charge for copies if requested.

Responsible Authority

The responsible authority and data practices compliance official for compliance under the Minnesota Data Practices Act is the city clerk. Designees in each department have been identified in the **Public Notice for Data Practices Act**.

Access to Public Data

All information maintained by the City is public unless a specific statutory designation gives it a different classification.

A. People Entitled to Access. Any person has the right to inspect and copy public data. Any person also has the right to have an explanation of the meaning of the data. Persons need not state their names or give reasons for their request.

B. Form of Request. Requests for public data may be verbal or written. Written requests are encouraged to best understand the data being requested.

C. Time Limits.

- **Requests**. Requests will be received and processed during normal business hours.
- **Response**. If copies cannot be made at the time of the request, copies will be supplied as soon as reasonably possible. Release of data may be done

either by arranging a time/date for inspection, data pickup, mail, or email, depending on the data format. Reasonable is defined by organizational issues (staffing hours of operation, etc.) and not by the person or entity making the request when he/she/it is not the subject of the data. Upon receiving a request staff may clarify what data is being requested. If the city does have the data but cannot provide it based on data practices classifications (private data for example), the city will notify the requestor as soon as reasonably possible and identify the law that prevents the release of the data. Response time may be impacted based on the size and/or complexity of the request as well as the number of requests in a given time period. The Data Practices Act does not require cities to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if the data is not kept in that form or arrangement. For example, if the data requested is only in paper form the city is not required to create electronic documents to respond to a request. If the city agrees to create data in response to a request there may be a fee charged.

D. Charging Members of the Public for Copies of Government Data

Minnesota Statutes, section 13.03, subd. 3(C) allows, but does not require, government entities to charge for copies of government data. A government entity cannot charge to separate public from not public data.

For 100 or fewer paper copies – 25 cents per page

100 or fewer pages of black and white, letter or legal size paper copies cost 25¢ for a one-sided copy, or 50¢ for a two-sided copy.

Most other types of copies – actual cost

The charge for most other types of copies, when a charge is not set by statute or rule, is the actual cost of searching for and retrieving the data, and making the copies or electronically sending the data. In determining the actual cost of making copies, the cost will include employee time, cost of the materials onto which the data is copied to (paper, CD, DVD, etc.), and mailing costs (if any). If the request is for copies of data that cannot be copied, such as photographs, the city may charge the actual cost of an outside vendor for the copies. In calculating employee time to make copies, it is based on the lowest-paid employee's wage (including benefits) who can make the copies. If it is necessary for a higher-paid employee to search/retrieve the data, the city will calculate search and retrieval charges at the higher wage. Estimates will be provided prior to gathering the data and will require payment prior to release of the data.

Access to Data on Individuals

Information about individuals is classified by law as public, private, or confidential. A list of private and confidential information is maintained in the City Clerk's Office.

Summary reports of data inventories by department contains items that are classified as public, private and confidential.

People Entitled to Access

Public information about an individual may be shown or given to anyone.

Private information about an individual may be shown or given to:

- The individual, but only once every six months, unless a dispute has arisen or additional data has been collected.
- A person who has been given access by the express written consent of the data subject.
- People who are authorized access by the federal, state, or local law or court order.
- People whom the individual was advised at the time the data was collected. The identity of those people must be part of the *Tennessen* warning described on page 16.
- People within the city staff, the City Council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

Confidential information may not be given to the subject of the data, but may be shown or given to:

- People who are authorized access by federal, state, or local law or court order.

Access to Data on Individuals (continued)

Form of Requests. Any individual may request verbally or in writing if the city has stored data about that individual and whether the data is classified as public, private, or confidential.

All requests to see or copy private or confidential information must be in writing. An **Information Disclosure Request** must be completed to document who requests and who receives this information. The responsible authority or designee must complete the relevant portion of the form. The responsible authority or designee may waive the use of this form if there is other documentation of the requesting party's identity, the information requested, and the city's response.

Identification of Requesting Party. The responsible authority or designee must verify the identity of the requesting party as a person entitled to access of non-public data. This can be through personal knowledge, presentation of written identification, comparison of the data subject's signature on a consent form with the person's signature in city records, or other reasonable means.

Time Limits.

- **Requests**. Requests will be received and processed during normal business hours.

- **Response**. The response must be immediate, if possible, or within 10 days if an immediate response is not possible.

Fees. Fees may be charged in the same manner as for public information.

Summary Data. Summary data is statistical records and reports derived from data on individuals but which does not identify an individual by name or any other characteristic that could uniquely identify an individual. Summary data derived from private or confidential data is public. The responsible authority or designee will prepare summary data upon request, if the request is in writing and the requesting party pays for the cost of preparation. The responsible authority or designee must notify the requesting party about the estimated costs and collect those cost before preparing or supplying the summary data. This should be done within 10 days after receiving the request. If the summary data cannot be prepared within 10 days, the responsible authority must notify the requester of the anticipated time schedule and the reasons for the delay.

Summary data may be prepared by redacting personal identifiers, redacting portions of the records that contain personal identifiers, programming computers to delete personal identifiers, or other reasonable means.

The responsible authority or designee may ask an outside agency or person to prepare the summary data if (1) the specified purpose is given in writing, (2) the agency or person agrees not to disclose the private or confidential data, and (3) the responsible authority determines that access by this outside agency or person will not compromise the privacy of the private or confidential data.

Juvenile Records

The following applies to *private* (not confidential) data about people under the age of 18.

- **Parental Access**. In addition to the people listed above who may have access to private data, a parent may have access to private information about a juvenile data subject. "Parent" means the parent or guardian of a juvenile data subject, or individual acting as a parent or guardian in the absence of a parent or guardian. The parent is presumed to have this right unless the responsible authority or designee has been given evidence that there is a state law, court order, or other legally binding document, which prohibits this right.

- **Notice to Juvenile**. Before requesting private data from juveniles, City personnel must notify the juveniles that they may request that the information not be given to their parent(s). This notice should be in the form attached as Appendix F, Exhibit 4.

- **Denial of Parental Access**. The responsible authority or designee may deny parental access to private data when the juvenile request this denial and the responsible authority or designee determines that withholding the data would be in the best interest of the juvenile. The request from the juvenile must be in writing stating the reasons for the request. In determining the best interest of the juvenile, the responsible authority or designee will consider:

    - Whether the juvenile is of sufficient age and maturity to explain the reasons and understand the consequences**.**

- Whether denying access may protect the juvenile from physical or emotional harm.

- Whether there are reasonable grounds to support the juvenile's reasons.

- Whether the data concerns medical, dental, or other health services provided under Minnesota Statues Sections 144.341 to 144.347. If so, the data may be released only if failure to inform the parent would seriously jeopardize the health of the minor.

The responsible authority or designee may also deny parental access without a request from the juvenile under Minnesota Statues Section 144.335.

Denial of Access

If the responsible authority or designee determines that the requested data is not accessible to the requesting party, the responsible authority or designee must inform the requesting party orally at the time of the request or in writing as soon after that as possible. The responsible authority or designee must give the specific legal authority, including statutory section, for withholding the data. The responsible authority or designee must place an oral denial in writing upon request. This must also include the specific legal authority for the denial.

Collection of Data on Individuals (M.S. §13.05, subd. 3)

The collection and storage of information about individuals will be limited to that necessary for the administration and management of programs specifically authorized by the state legislature, city council, or federal government.

When an individual is asked to supply private or confidential information about the individual, the City employee requesting the information must give the individual a *Tennessen* warning. This warning must contain the following:

- The purpose and intended use of the requested data, whether the individual may refuse, or is legally required to supply the requested data

- Any known consequences from supplying or refusing to supply the information

- The identity of other persons or entities authorized by state or federal law to receive the data

A *Tennessen* warning is not required when an individual is requested to supply investigative data to a law enforcement officer.

A *Tennessen* warning may be on a separate form or may be incorporated into the form, which requests the private or confidential data.

Challenge to Data Accuracy (M.S. §13.04, subd. 4)

An individual who is the subject of public or private data may contest the accuracy or completeness of that data maintained by the city. The individual must notify the responsible authority in writing describing the nature of the disagreement. Within 30 days, the responsible authority or designee must respond and either (1) correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual, or (2) notify the individual that the authority believes the data to be correct.

An individual who is dissatisfied with the responsible authority's action may appeal to the Commissioner of the Minnesota Department of Administration, using the contested case procedures under Minnesota Statues Chapter 14. The responsible authority will correct any data if so ordered by the Commissioner.

Data Protection

A. Accuracy and Currency of Data.

- All employees will be required, and given appropriate forms, to provide updated personal information to the appropriate supervisor, Human Resources Director, or Finance Director, which is necessary for tax, insurance, emergency notification, and other personnel purposes. Other people who provide private or confidential information will also be encouraged to provide updated information when appropriate.

- Department heads should periodically review forms used to collect data on individuals to delete items that are not necessary and to clarify items that may be ambiguous.

- All records shall be disposed of according to the City's Records Retention Schedule.

B. Data Safeguards.

- Private information will be stored in files or databases which are not readily accessible to individuals who do not have authorized access and which will be secured during hours when the offices are closed.

- Private data will be kept only in City offices only, except when necessary for use outside of offices for city business.

- Only those employees whose job responsibilities require them to have access will be allowed access to files and records that contain private information. These employees will be instructed to:

    - Not discuss, disclose, or otherwise release private data to City employees whose job responsibilities do not require access to the data

    - Not leave private data where non-authorized individuals might see it

    - Shred private data before discarding

    - When a contract with an outside party requires access to private or confidential information, the contracting party will be required to use and disseminate the information consistent with the Minnesota Data Privacy Act.

Police Department. The police department has detailed data practices plan relating to law enforcement. This is titled "Blaine Police Department General Order 318.0."

SECTION III – POLICY STATEMENTS

Records Destruction Policy

The city has contracted with a vendor to dispose of sensitive and private data. Shredding the documents will complete the disposal of this material. Bins/counsels are located in the police department, building inspections, administration and community standards areas of City Hall. Documents, CD-ROMs, CD-Rs, DVDs and any other material containing confidential and/or private data will be placed in these containers. The vendor services the consoles on a regular basis for shredding on-site.

Back-Up Policy

The city's information technology department has implemented a policy for service/backing up the computer network.

Email/Internet/Social Media/Computer Use Policies

Email, internet, social media, and computer use policies are all covered under the use of city equipment/facility and social media/social networking policies.

Tennessen Warning/Informed Consent Policy

When a government entity collects private or confidential data from an individual about the individual, the entity must give the individual a Tennessen warning notice (Minnesota Statutes, section 13.04, subdivision 2). The Tennessen warning notice must include how the entity intends to use the data and which outside entities or persons are authorized to have the data. Once the entity gives the notice, the entity may use or release the data in the ways described in the notice.

After giving a Tennessen warning and collecting private data from an individual, a government entity may wish to use the data differently than it described, or may wish to release the data to an outside entity (government or non-government) or person other than it described. In either of these situations, the government entity would need to obtain informed consent from the individual.

Ensuring the Security of Not Public Data Policy

Legal Requirement

The adoption of this policy by the City of Blaine satisfies the requirement in Minnesota Statutes, section 13.05, subd. 5, to establish procedures ensuring appropriate access to not public data. By incorporating employee access to not public data in the City of Blaine's data inventory (required by Minnesota Statutes, section 13.025, subd. 1), in the individual employee's position description, or both, the city's policy limits access to not public data to employees whose work assignment reasonably requires access.

Please direct all questions regarding this policy to the City's Data Practices Compliance Official (DPCO):

Catherine Sorensen
City Clerk
10801 Town Square Drive NE
Blaine MN 55449
763-785-6122
csorensen@blainemn.gov

Procedures Implementing this Policy

Definitions

Confidential or protected nonpublic data are available only to those government employees who require access to it for work-related reasons, or others who are specifically authorized by law.

Data Inventory

Under the requirement in Minnesota Statutes, section 13.025, subd. 1, the city has prepared a data inventory which identifies and describes all not public data on individuals maintained by the city. To comply with the requirement in section 13.05, subd. 5, the city has also modified its data inventory to represent the employees who have access to not public data.

In the event of a temporary duty as assigned by a manager or supervisor, an employee may access certain not public data, for as long as the work is assigned to the employee.

In addition to the employees listed in the city's data inventory, the responsible authority, the data practices compliance official, the city's management team and city attorney may have access to all not public data maintained by the city if

necessary for specified duties. Any access to not public data will be strictly limited to the data necessary to complete the work assignment.

Employee Position Descriptions
Position descriptions may contain provisions identifying any not public data accessible to the employee when a work assignment reasonably requires access.

Data Sharing With Authorized Entities or Individuals
State or federal law may authorize the sharing of not public data in specific circumstances. Not public data may be shared with another entity if a federal or state law allows or mandates it. Individuals will have notice of any sharing in applicable Tennessen warnings (see Minnesota Statutes, section 13.04) or the city will obtain the individual's informed consent. Any sharing of not public data will be strictly limited to the data necessary or required to comply with the applicable law.

Ensuring That Not Public Data are Not Accessed Without a Work Assignment
Within the city divisions may assign tasks by employee or by job classification. If a division maintains not public data that all employees within its division do not have a work assignment allowing access to the data, the division will ensure that the not public data are secure. This policy also applies to divisions that share workspaces with other divisions within the city where not public data are maintained.

Recommended actions for ensuring appropriate access include:

- Assigning appropriate security roles, limiting access to appropriate shared network drives, and implementing password protections for not public electronic data
- Password protecting employee computers and locking computers before leaving workstations
- Securing not public data within locked work spaces and in locked file cabinets
- Shredding not public documents before disposing of them

Penalties for Unlawfully Accessing Not Public Data
The city will utilize the penalties for unlawful access to not public data as provided for in Minnesota Statutes, section 13.09, if necessary. Penalties include suspension, dismissal, or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

Public Notice for Data Practices Act
November 2019

PURSUANT to Minnesota Statutes, §13.05, the Minnesota Government Data Practices Act, the responsible authority for the City of Blaine is:

CATHERINE M. SORENSEN
CITY CLERK
10801 TOWN SQUARE DRIVE
BLAINE MN 55449
(763) 784-6700
csorensen@blainemn.gov

PURSUANT to Minnesota Statutes, §13.05, the Minnesota Government Data Practices Act, the data practices compliance official for the City of Blaine is:

CATHERINE M. SORENSEN
CITY CLERK
10801 TOWN SQUARE DRIVE
BLAINE MN 55449
(763) 784-6700
csorensen@blainemn.gov

Inquiries regarding government data created, maintained or disseminated by the city can also be directed to identified designees.

The General Records Retention Schedule includes private or confidential data on individuals maintained by the city (see Minn. Stat. 13.05 and Minn. Rules 1205.1200). The City of Blaine's procedures described throughout this entire policy is intended to ensure that not public data are only accessible to individuals whose work assignment reasonably requires access (see Minn. Stat. 13.0, subd. 5). In addition to any designated employees, the city's responsible authority, data practices compliance official, management team and city attorney may also have access to all not public data on an as needed basis as part of a specific work assignment.