

City of Northfield, Minnesota

Guidelines and Procedures For the Minnesota Government Data Practices Act

“Responsible Authority” and “Compliance Official”

Deb Little, City Clerk
801 Washington Street
Northfield, MN 55057

Subject

1.	Introduction	4
2.	Responsible Authority	4
3.	Classifications of Data on Individuals	4
	A. Public Data	4
	B. Private Data	4
	C. Confidential Data	4
4.	Access to Public Data	5
	A. People Entitled to Access	5
	B. Form of Request	5
	C. Questions of Requesting Parties	5
	D. Time Limits	5
	E. Fees	5
5.	Access to Data on Individuals	6
	A. People Entitled to Access	6
	B. Form of Request	7
	C. Identification of Requesting Party.....	7
	D. Time Limits	8
	E. Fees	8
	F. Summary Data	8
	G. Juvenile Records	8
6.	Denial of Access	9
7.	Collection of Data on Individuals	10
8.	Challenge to Data Accuracy	10
9.	Data Protection	11
	A. Accuracy and Currency of Data	11
	B. Data Safeguards	11

Exhibits (Incorporated as a reference only – subject to updates & changes)

1.	List of Designated Employees	12
2.	Data Request Form	13
3.	Consent for the release of information.....	14
4.	Disclosure & release of information	15
5.	Government Data Access and Non-Disclosures Agreement	16
6.	Notice to Persons Under Age of 18	18
7.	Data Practices Advisory	19
8.	Sample Contract Provision	20

Appendix

Data Collected by the City	A
City Forms Used to Collect Data	B

1. Introduction.

These procedures are adopted to comply with the requirements of the Minnesota Data Practices Act (the Act), specifically Minn. Stat. Sec. 13.03, Subd. 2 and 13.05, Subd. 5 and 8.

2. Responsible Authority and Data Practices Compliance Official.

The person who is the responsible authority and data practices compliance official under the Act is Deb Little, City Clerk, 801 Washington Street, Northfield, MN 55057. The data practices compliance official is the city employee to whom persons may direct questions or concerns regarding problems in obtaining access to information. The responsible authority has designated certain other city employees to assist in complying with the Act. These designees are listed on attached Exhibit 1.

3. Classifications of Data on Individuals.

Data on individuals is “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.” “Individual” is defined as a living human being. There are three types of data on individuals: public, private, and confidential. The Act includes two additional classifications, “data not on individuals” and “data on decedents”, but because data in these additional classifications are less frequently requested they are not explained in this document.

- A. Public Data.** Public data is data on individuals that is not classified by state statute, federal law or temporary classification as either private or confidential. It is accessible to anyone for any reason.
- B. Private Data.** Private data is any data on individuals that is not accessible to the public, but is accessible to the subject of the data. Private data includes data that is expressly classified as private by state statute, federal law, or temporary classification.
- C. Confidential Data.** Confidential data is data on individuals that is not accessible to the subject of the data or to the public. It includes data that is expressly classified as confidential by state statute, federal law or temporary classification.

4. Access to Public Data.

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

- A. People Entitled to Access.** Any person has the right to inspect and copy public data. The person also has the right to have an explanation of the meaning of the data. The person does not need to state his or her name or give the reason for the request.
- B. Form of Request and Response.**
- **Request.** The request for public data may be verbal or written.
 - **Response.**
 - The city is not required to provide information verbally over the telephone.
 - The city may provide information by fax or e-mail, at its own discretion.
 - The city is not required to provide information in any specific format, except that if the data is maintained in electronic format and is requested to be electronic format, then it must be provided in that medium. This does not mean that the city will provide the data in an electronic format or program that is different from what the city has.
- C. Questions of Requesting Parties.** People requesting public data must not be asked to identify themselves or state a reason for the request. They may be asked to provide certain identifying or clarifying information for the sole purpose of facilitating access to the data.
- D. Time Limits.**
- **Requests.** Requests will be received and processed only during normal business hours.
 - **Response.** If copies cannot be made at the time of the request, copies must be supplied as soon as reasonably possible.
- E. Fees.** Fees may be charged only if the requesting person asks for a copy or electronic transmittal of the data. Fees will be charged according to the City's fee schedule as amended from time to time by the City Council, unless significant time is required. In that case, the fee will include the actual cost of searching for,

retrieving, and copying or electronically transmitting the data. The fee may not include time necessary to separate public from non-public data.

The responsible authority may also charge an additional fee if the copies have commercial value and are a substantial and discrete portion of a formula, compilation, program, process, or system developed with significant expenditure of public funds. This additional fee must relate to the actual development costs of the information.

5. Access to Data on Individuals.

Information about individual people is classified by law as public, private, or confidential. A list of the private and confidential information maintained by the City is contained in Appendix A (on file in the City Clerk's office). The forms used to collect private and confidential information are contained in Appendix B (on file in the City Clerk's office).

A. 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 subject, 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. This consent must be on the form attached as Exhibit 3, or a form reasonably similar.
 - People who are authorized access by federal, state, or local law or court order.
 - People about whom the individual was advised at the time the data was collected. The identity of those people must be part of the *Tennessee* warning described below.
 - 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.
- People within the city staff, the city council, and outside agents (such as attorneys) whose work assignments or responsibilities reasonably require access.

B. Form of Request and Response.

- **Request.** 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*, attached as Exhibit 2, must be completed to document who requests and who receives this information. The responsible authority or designee must complete the relevant portions 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.

- **Response.**
 - The city is not required to provide information verbally over the telephone.
 - The city may provide information by fax or e-mail, at its own discretion.
 - The city is not required to provide information in any specific format, except that if the data is maintained in electronic format and is requested to be electronic format, then it must be provided in that medium. This does not mean that the city will provide the data in an electronic format or program that is different from what the city has.
 - Requests for names and addresses of residents must be made in person or in writing.

- C. Identification of Requesting Party.** The responsible authority or designee must verify the identity of the requesting party as a person entitled to access. 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.

D. Time Limits.

- **Requests.** Requests will be received and processed only during normal business hours.
- **Response.** The response must be immediate, if possible, or within 10 days (excluding Saturdays, Sundays and legal holidays) if an immediate response is not possible.

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

F. 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 costs 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 “blacking out” personal identifiers, cutting out portions of the records that contain personal identifiers, programming computers to delete personal identifiers, or other reasonable means.

The responsible authority may ask an outside agency or person to prepare the summary data if (1) the specific 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. The responsible authority may use the form attached as Exhibit 5.

G. 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 Exhibit 6.

- **Denial of Parental Access.** The responsible authority or designee may deny parental access to private data when the juvenile requests 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 is reasonable grounds to support the juvenile’s reasons, and
 - Whether the data concerns medical, dental, or other health services provided under Minnesota Statutes 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 city complies with all HIPPA requirements.

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

6. 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.

7. Collection of Data on Individuals.

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 *Tennessee* 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, and
- the identity of other persons or entities authorized by state or federal law to receive the data.

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

A *Tennessee* warning may be on a separate form or may be incorporated into the form which requests the private or confidential data. See attached Exhibit 7.

8. Challenge to Data Accuracy.

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 city's 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 Statutes Chapter 14. The responsible authority will correct any data if so ordered by the Commissioner.

9. Data Protection.

A. Accuracy and Currency of Data.

- All employees will be requested, and given appropriate forms, to provide updated personal information to the appropriate staff person, 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 must be disposed of according to the city's records retention schedule.

B. Data Safeguards.

- Private and confidential 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 and confidential data must be kept only in city offices, except when necessary 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 or confidential information. These employees will be instructed to:
 - not discuss, disclose, or otherwise release private or confidential data to city employees whose job responsibilities do not require access to the data,
 - not leave private or confidential data where non-authorized individuals might see it, and
 - shred private or confidential 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 Act. The city may include in a written contract the language contained in Exhibit 8.