

POLICIES FOR THE MINNESOTA GOVERNMENT DATA PRACTICES ACT
for the CITY OF BLOOMINGTON, MINNESOTA

Effective August 1, 2022

TABLE OF CONTENTS

Introduction 3

 I. Classification of Data..... 4

 II. Definitions..... 6

 III. Public Data Access Policy 9

 IV. Data Subjects Rights and Access Policy 12

 V. Policy for Ensuring the Security of Not Public Data 15

 VI. Contractor Compliance 17

Appendix A: Data Inventory

Appendix B: General Data Access Request Form

Appendix C: Form for Denial of Parental Access to Data Request

Appendix D: Copy Costs

Introduction

The Minnesota Government Data Practices Act (“MGDPA” or the “Act”), Minnesota Statutes Chapter 13, regulates all data collected, received, maintained, disseminated, or stored by a state agency, political subdivision, or state-wide system. The City of Bloomington is subject to all provisions of the Act.

Minnesota Statutes §§ 138.161-138.225 governs the retention, storage, and disposition of government data. The City of Bloomington is subject to these provisions.

The City of Bloomington has established a Records Retention Schedule which complies with these and other relevant data management controls.

The City of Bloomington has established a Fee Schedule related to the retrieval and collection of data in response to requests made pursuant to the Act. See [Appendix D](#).

Pursuant to Minnesota Statutes § 13.025, subd.1, the City of Bloomington has prepared a **Data Inventory** with a description of each category of record, file, or process related to private or confidential data on individuals maintained by the City. This inventory is located herein at [Appendix A](#).

Further, pursuant to Minnesota Statutes § 13.025, subds. 2 and 3, the City of Bloomington has established the **Public Data Access Policy** and the **Data Subject Rights and Access Policy** as set forth herein (the “Policies”).

I. Classification of Data

A. Permanent Classifications.

Unless otherwise designated by the Act, other applicable statute, or temporary classification, all data that is collected, created, received, maintained, or disseminated by the City is presumed to be public. This includes all data, regardless of format. This includes, but is not limited to paper, email, flash/thumb drives, external hard drives, CDs, DVDs, microfiche, and photographs.

Pursuant to the Act, all government data is divided into three general classifications: (1) data on individuals; (2) data not on individuals; and (3) data on decedents. Each classification has three subcategories that determine who may access data. Data on individuals and data on decedents is either public, private, or confidential; data not on individuals is either public, nonpublic, or protected nonpublic.

In all three classifications, public data is accessible by anyone.

Private data on individuals and private data on decedents is accessible by a data subject and government employees and officials with a business need to know; similarly, nonpublic data not on individuals is accessible by a data subject and government employees and officials with a business need to know.

Confidential data on individuals and confidential data on decedents is accessible by only government employees and officials with a business need to know; similarly, protected nonpublic data is accessible by only government employees and officials with a business need to know.

The League of Minnesota Cities developed the following chart for clarity:

Data on Individuals	Data Not On Individuals	Data On Decedents	Who Has Access
Public	Public	Public	Anyone
Not Public			
Private	Nonpublic	Private	Data Subjects and government employees and officials with a business need to know
Confidential	Protected Nonpublic	Confidential	Only government employees and officials with a business need to know

B. Temporary Classifications.

When a city has a compelling reason to want to protect certain data or certain types of data that would otherwise be presumed to be public, a city may request that the Commissioner of Administration create a temporary classification of that data or type of data. The city must apply to the Department of Administration using the Department's approved form; the application by the city is public data.

C. Changing Data Classifications.

The same data may fall into more than one category, depending on the timing or use of the data. For example, certain criminal investigative data is confidential or protected nonpublic until the investigation becomes inactive as defined by the Act; once the investigation is inactive, that same data becomes public.

The Legislature alone has the authority to amend the Act to change the classification of data.

II. Definitions

When used in this document, the following terms have these meanings:

Responsible Authority is Christina M. Scipioni, City Clerk for the City of Bloomington. The duties of the Responsible Authority include controlling the collection, use, and dissemination of government data. The Responsible Authority is charged with classifying, maintaining, and securing City government data; responding to data requests; resolving disputes related to data; and all other duties set forth in the Act. A new resolution must be adopted if this appointment changes.

The Responsible Authority may designate one or more Designees (as defined below) and must instruct all Designees in the requirements of the Act and applicable Rules. The Responsible Authority must appoint a Data Practices Compliance Official (as defined below).

The Responsible Authority for the City of Bloomington may be contacted at:

City of Bloomington
1800 West Old Shakopee Road
Bloomington, MN 55431
952-563-4989
cmscipioni@bloomingtonmn.gov

Designee means any person designated by the Responsible Authority to be in charge of individual files or systems containing government data, and to receive and comply with data requests. A Designee must be a City employee, and must be appointed by written order.

Data Practices Compliance Official means the person who is responsible for responding to questions or concerns regarding the Act. The Data Practices Compliance Official is Marla Oakland, Deputy City Clerk/Records Manager, and may be contacted at:

City of Bloomington
1800 West Old Shakopee Road
Bloomington, MN 55431
Phone: 952-563-4728
Email: moakland@bloomingtonmn.gov

City means the City of Bloomington, a Minnesota municipal corporation.

Government Data means all data created, collected, received, maintained, or disseminated by any state agency, political subdivision, or statewide system regardless of the data's physical form, storage media or conditions of use. Government data includes all papers, cards, correspondence, discs, maps, memoranda, microfilm, photographs, recordings, reports, tapes, writings, computer medium and other data, information, or documentary material. Data collected must be accurate, complete, and current for the purposes for which it was collected.

Data Subject means a person who can be identified from certain Government Data.

Data on individuals means all data in which any individual is or can be identified as the subject of the 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.

Public data on individuals is data on individuals, living or dead, which is accessible to the public. Unless classified otherwise by state or federal law or temporary classification, all data on individuals is accessible to the public regardless of its interest in the data.

Private data on individuals is data, which is not accessible to the public, but is accessible to the data subject. Data on individuals is private if so, classified by state or federal law or temporary classification. In addition to the data subject, private data is also accessible to the data subject's representative, individuals, entities, or persons given express written permission by the data subject, a minor's parent or guardian, personnel within the governmental entity whose work assignments reasonably require access, individuals, entities, or persons authorized by state or federal law, and pursuant to a court order.

Private data on decedents means data which, prior to the death of a data subject, were classified by state or federal law or temporary classification as private data. Private data on decedents is accessible to the representative of the decedent, the trustee appointed in a wrongful death action, individuals, entities, or persons given express written permission by the data subject, or the representative of the decedent, persons, individuals, or entities authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order. Private data on decedents is public ten years after the actual or presumed death of the data subject and thirty years after the creation of the data.

Confidential data on individuals means data which by state or federal law or temporary classification is not accessible to the public or to the subject of the data. Confidential data on individuals is accessible to individuals authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order.

Confidential data on decedents means data which, prior to the death of a data subject, were classified by state or federal law or temporary classification as confidential data. Confidential data on decedents is accessible to individuals authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order. Confidential data on decedents is public ten years after the actual or presumed death of the data subject and thirty years after the creation of the data.

Public data not on individuals is data accessible to the public unless otherwise classified by state or federal law or temporary classification.

Nonpublic data not on individuals means data which is not public but is accessible to the subject of the data, if any. As used here, the "subject of the data" means an individual, partnership, corporation, or other legal entity. Data not on individuals is nonpublic if so, classified by state or federal law or temporary classification. Nonpublic data is accessible to the subject of the data, if

any, and to individuals, entities or persons authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order. However, nonpublic data not on individuals may be discussed at a meeting open to the public to the extent allowed by the Open Meeting Law (see Minnesota Statutes § 13D.05). Except for security information, nonpublic data shall become public ten years after the data was created, collected, or received by the governmental agency. Access may be denied if release of the data will result in harm to the public or data subject when such harm outweighs the benefit to the public.

Protected nonpublic data not on individuals means data which is not public and not accessible to the subject of the data. Data not on individuals is protected nonpublic if so classified by state or federal law or temporary classification. Protected nonpublic data is accessible to individuals, entities or persons authorized by state or federal law, personnel within the entity whose work assignments reasonably require access, and pursuant to a court order. Except for security information, protected nonpublic data shall become public ten years after the data was created, collected, or received by the governmental agency. Access may be denied if release of the data will result in harm to the public or data subject when such harm outweighs the benefit to the public.

Summary data means statistical records and reports derived from data on individuals but in which the individuals are not in any way identifiable. Summary data is public data unless otherwise classified by state or federal law or temporary classification.

III. Public Data Access Policy

Pursuant to Minnesota Statutes § 13.025, the City of Bloomington has established this **Public Data Access Policy**.

A. Right to Access Public Data.

All Government Data (see definition above), regardless of its format, is presumed to be public, unless the Act or other applicable law says otherwise. The Act also requires the City to maintain and store Government Data in a way that makes it easily accessible by members of the public.

Members of the public have the right to look at (inspect), without charge, all public data that the City keeps, and to be informed of its meaning if there are technical terms not commonly understood. The City is not obligated to create new data in response to a data request.

Members of the public also have the right to obtain copies of public data. The City is allowed to charge members of the public for copies (see [Appendix D](#)), but members of the public may inspect the data before deciding to request copies.

B. How to Make a Data Request.

A member of the public may make a request for Government Data online through the City's [Data Practices Center](#), in person, or in writing. For written requests, the City requests that members of the public to submit the General Data Access Request form for data requests (see [Appendix B](#)). If a member of public chooses not to use the Data Practices Center or data request form, the request must be in writing and include: (1) a clear statement that a data request is being made pursuant to the Minnesota Government Data Practices Act; (2) whether the requestor wishes to inspect the data, or have copies, or both; and (3) a clear description of the data that is being requested.

The City cannot require a member of the public to show identification or explain the reason for the data request. However, City staff may ask for identification information to (1) verify whether a requestor is the subject of the requested data in order to access private or nonpublic data or (2) to obtain sufficient information for mailing the requested data (via U.S. Mail or electronic transmission). If a requestor does not want to give identifying information, the requestor may request contact information from City staff with whom the requestor may communicate regarding the status of the data request.

C. How the City Responds to a Data Request.

Upon receipt of a request, the Responsible Authority, Data Practices Compliance Official, or Designee will acknowledge such receipt, attempt to clarify anything that is

unclear about the request, and if applicable, provide notice about the costs of supplying data and the City's requirement to prepay.

1. *Process when Requestor is the Subject of the Data.*

If the City has the data and it is public or private data about the requestor, the City will respond to the request within 10 business days by either:

- a. Providing the data through the City's [Data Practices Center](#); or
- b. Arranging for a time, date, and place for the requestor to inspect the data, for free, if the requestor has asked to inspect the data; or
- c. Providing the copies of the data as requested. The requestor may choose to pick up the copies, or the copies will be mailed or faxed to the requestor. The City will provide electronic copies (e.g., email) upon request, if the data is maintained in electronic format.

If the City has the data, but the data is confidential or private data that is not about the requestor, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor within 10 business days and will notify the requestor of the specific laws that prevent the requestor from accessing the data.

2. *Process when Requestor is not the Subject of the Data.*

If the City has the data, and the data is public, the Responsible Authority, Data Practices Compliance Official, or Designee will respond to the requestor as soon and reasonably possible. Requests for public data where the requestor is not the subject of the data will be handled on a first-come, first-served basis, depending on the scope and volume of the request and as staff time and resources will allow. When the public data is compiled and available, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor of its availability by either:

- a. Providing the data through the City's [Data Practices Center](#); or
- b. Arranging for a time, date, and place for the requestor to inspect the data, for free, if the requestor has asked to inspect the data; or
- c. Providing the copies of the data as requested. The requestor may choose to pick up the copies, or the copies will be mailed or faxed to the requestor. The City will provide electronic copies (e.g., email) upon request, if the data is maintained in electronic format.

If the City has the data, but the data is not public, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor as soon as reasonably possible that the data is not public and will notify the requestor of the specific laws that prevent the requestor from accessing the data.

Information about copy costs are set forth in [Appendix D](#).

If the requestor of the data does not understand the meaning of the data (e.g., technical terminology, abbreviations, acronyms, jargon, etc.), the requestor may ask for an explanation of the meaning of the data. The City is not required to respond to questions that are not specific requests for data.

The City will not, and is not obligated to, create data or collect new data in response to a request. The City will not, and is not obligated to, provide the requested data in any specific form or arrangement if the data is not already maintained in that form or arrangement.

D. Requests for Summary Data.

Summary Data ([see definition above](#)) is available, but the City is not obligated to create new data in response to a request for summary data. The City will decide whether it will create summary data or decline to create summary data. Summary data is not a means to gain access to private or confidential data.

IV. Data Subjects Rights and Access Policy

Pursuant to Minnesota Statutes § 13.025, the City of Bloomington has established this **Data Subjects Rights and Access Policy**. This policy applies only to those people or entities who are the subject of data that is collected, maintained, and/or disseminated by the City.

A. Data Subjects

In the normal course of business, the City collects, maintains, and disseminates Government Data (see definition above) from members of the public, public and private entities, its employees, and others who interact with the City. The Act governs the rights that data subjects have related to the data that the City collects, maintains, and disseminates. The City has established procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected. The City has further established procedures for ensuring that data that are not public are only accessible to persons whose work assignments reasonably requires access to the data and is only being accessed by those persons for purposes for which the data was collected and pursuant to these Policies.

B. Classification of Data About Data Subjects

All Government Data is presumed to be public, unless another state or federal law classifies the data as not public.

1. *Public data.* The City is obligated to give public data to anyone who asks for it, regardless of the requestor's purpose or proposed use of the data. Example, the name and address information of a person who addresses the City Council at a public hearing is public data.
2. *Private data.* The City is not allowed to give to the general public any private data about a data subject; only the subject of the data has access to this data. The City is allowed to share this data with the subject of the data, a representative that the data subject has designated, or with a City employee or agent whose work for the City requires access to the data. Example, a data subject's Social Security Number.
3. *Confidential data.* The City is not allowed to give confidential data to anyone, not even the data subject. The City may share this data only with a City employee or agent whose work for the City requires access to the data. Example, data about a data subject who is part of an active police investigation.

See above section I. above for more information about the classifications of data.

C. Data Subjects' Rights Under the Act

1. Access

Data subjects have the right to inspect public and private Government Data about themselves. This inspection must be available at no cost to the data subject. Data subjects may also have copies of the public and private data about themselves, and the City is allowed to charge for these copies. A data subject may inspect the data before deciding whether or not request copies of all or part of the data.

Upon request, the City is required to inform a data subject about the classification of data that the City maintains on that data subject.

Parents have the right to inspect or get copies of the public and private data that the City collects, maintains, or disseminates about the parent's minor child(ren). Legal guardians have this same right related to the minors for whom they are appointed as guardian.

Minors (children under 18) have the right to request that the City not give out their public or private data, and the City is required to inform a minor of this right. The City requires the minor to put the request in writing on the Denial of Parental Access to Data Request form attached as [Appendix C](#) (or access the form [here](#)). The City does have the authority to deny such a request based on the minor's best interests. Minors do not have the right to make this request if the data at issue is educational data maintained by an educational agency or institution.

2. When the City Collects Data

When the City requests that a data subject provide data that is not public data, the City must give the data a notice, usually referred to as a *Tennessee Warning*. This notice gives a data subject information about why the City is collecting certain data, what the intended use of that data will be, and limits what the City can do with the data. The City cannot use or release the data for a purpose other than the purpose for which it was collected. The City must obtain written permission ("informed consent") from a data subject before the City can use or release the data for any other purpose.

3. Data Security

The City is required to protect all not public Government Data. The City has established appropriate measures to ensure that all not public Government Data is safe. If the City determines that a security breach has occurred and an unauthorized person has accessed private or confidential data, the City is required to notify affected data subjects of the breach.

4. Challenging Accuracy and/or Completeness of Data

A data subject has the right to challenge the accuracy and/or completeness of the public and private data that the City maintains about that data subject. The data subject has the right to appeal any decision made on a challenge. A parent or guardian has the same rights related to the public or private data about the minor(s) for whom they are legally responsible.

D. Copy Costs

See [Appendix D](#).

E. Data Request Form

See [Appendix B](#).

V. Policy for Ensuring the Security of Not Public Data

A. Legal Requirement.

Pursuant to Minnesota Statutes § 13.05, subd. 5, the City of Bloomington has established this **Policy for Ensuring the Security of Not Public Data**. By incorporating employee access to not public data in the City's Data Inventory (required by Minnesota Statutes § 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 identified herein.

B. Procedures for implementing this policy.

1. Data inventory

Under the requirements of Minnesota Statutes § 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 Minnesota Statutes § 13.05, subd. 2, the City has also modified its Data Inventory to represent the employees with 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, Data Practices Compliance Official, the City's Executive Leadership Team ("ELT"), and the City Attorney and Legal Department staff 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.

2. Employee Position Descriptions

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

3. Data Sharing with Authorized Entities or Individuals

State or federal law or a court order 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 *Tennessee* warnings, 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.

4. Ensuring that Not Public Data are not Accessed Without a Work Assignment

Within the City, divisions or departments may assign tasks by employee or by job classification. If a division or department maintains not public data that all employees within its division or department do not have work assignment allowing access to the data, the division or department will ensure that the not public data are secure. This policy also applies to divisions or departments that share workspaces with other divisions or department 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 workspaces and in locked file cabinets
- Shredding not public data before disposing of them

5. 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 § 13.09, if necessary. Penalties include suspension, dismissal, or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

VI. Contractor Compliance

Generally, parties that contract with the City to perform services and other City functions are required to comply with all requirements of the Act if the outside entity has business access to Government Data, or otherwise collect, maintain or disseminate Government Data. The contractor may not release or disseminate any Government Data without written approval from the City. Upon termination of a contract, a contractor may be required to return all Government Data to the City as requested.

Appendix A
Data Inventory

File is too large to include within this document. Available upon request by contacting the City Clerk's Office at 952-563-4989.

Appendix B General Data Access Request Form



General Data Access Request

Government Data Practices Act

Requester

Notice: You may cancel this request at any time prior to the release of information.

Note: The subject of the data request must authorize the release of private information to the subject's agent or another agency. An "Informed Consent to Release" must be completed by the subject of the data.

You may be required to pay the actual costs of making and/or compiling data, if our request exceeds 100 pages. Smaller requests cost 25¢ per page.

Name	Last	First	M.I. (optional)	Date
Address	Street	City	State	Zip
				<i>(Only if data is to be sent by mail.)</i>
Information requested				Phone
				Email

Data Classification

Data classification *If data classification is unknown, consult Legal Department.*

Public
 Non-public
 Confidential
 Private

Request	<input type="checkbox"/> Approved <input type="checkbox"/> Approved in part <input type="checkbox"/> Denied	Authorized signature
---------	---	----------------------

Comments *Enter any appropriate remarks or comments. If data access is denied, cite authority or reason.*

Fees

Provide a receipt each time money is received.

Rate per page	25¢	X	Number of pages	=	\$	
			Other fees	+	\$	
			Subtotal	=	\$	
			Sales tax (7.275%)	+	\$	
			TOTAL DUE	=	\$	<i>If over \$50, prepay 50%.</i>
			Amount prepaid	-	\$	Date received _____
			Balance due	=	\$	Date received _____

Code to: _____ - _____ - _____ - _____

The City of Bloomington does not discriminate on the basis of disability in the admission or access to, or treatment or employment in, its services, programs or activities. Upon request, a reasonable accommodation will be provided to allow individuals with disabilities to participate in all City of Bloomington services, programs, and activities.

City Clerk's Office

1800 W. Old Shakopee Road
Bloomington MN 55431-3027
datarequests@BloomingtonMN.gov

PH 952-563-4989
FAX 952-563-4741
TTY 952-563-8740

BloomingtonMN.gov

web02_001 pg1 of 1 (07/17)

Appendix C

Denial of Parental Access to Data Request



Denial of Parental Access to Data Request

(Minor Data Subject)

I, _____, request the City of Bloomington
Name of minor (individual younger than 18 years)

to deny access to data concerning me that is considered private or confidential under Minnesota law, for the following reasons:

Signed this _____ day of _____ 20 _____.

Signature of minor individual

Date of birth

Subscribed and sworn to before me, a

Notary Public, on this _____ day

of _____ 20 _____.

Commission expires on _____.

Notary signature

The City of Bloomington does not discriminate on the basis of disability in the admission or access to, or treatment or employment in, its services, programs or activities. Upon request, a reasonable accommodation will be provided to allow individuals with disabilities to participate in all City of Bloomington services, programs, and activities.

City Clerk's Office

1800 W. Old Shakopee Road
Bloomington MN 55431-3027

PH 952-563-4989
FAX 952-563-4741
TTY 952-563-8740

BloomingtonMN.gov

wob22_006 pg1 of 1 (07/17)

Appendix D

Excerpt of City Fee Schedule for Copy Costs
See City website at <https://www.bloomingtonmn.gov/>

General Copies (data requests)	Paper copies - 100 or more pages, black and white, letter or legal sized paper copies ^(A)	\$.25 per page, plus \$35 per hour of staff time
	Paper copies - color	\$.60 per page, plus \$35 per hour of staff time
	Electronic copies - fewer than three hours of staff time ^(A)	No charge
	Electronic copies - three or more hours of staff time ^(A)	\$35/hour