

City of Bloomington Policies for the Minnesota Government Data Practices Act

Public Data Access Policy

Data Subjects Rights and Access Policy

Policy for Ensuring the Security of Not Public Data

Effective August 1, 2026

Table of Contents

Introduction -----	1
Definitions-----	2
Public Data Access Policy-----	5
Data Subjects Rights and Access Policy-----	8
Policy for Ensuring the Security of Not Public Data-----	12
Appendix A: Copy Costs-----	14
Appendix B: Classification of Data -----	15
Appendix C: Denial of Parental Access to Data Request -----	16
Appendix D: Informed Consent to Release -----	17
Appendix E: Standards for Verifying Identity -----	18

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.

The Act presumes that all government data are public and accessible by the public for both inspection and copying unless a state or federal law or a temporary classification makes the data not public.

Furthermore, pursuant to Minnesota Statutes § 13.025, 13.03, and 13.05 the City of Bloomington has established the Public Data Access Policy, the Data Subject Rights and Access Policy, and Policy for Ensuring the Security of Not Public Data as set forth herein (the “Policies”).

Definitions

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

Responsible Authority is designated by the Bloomington City Council and is responsible for 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 the Responsible Authority designation 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 is:

Marla Oakland
City of Bloomington
1800 West Old Shakopee Road
Bloomington, MN 55431
952-563-4728
moakland@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 responsible for responding to questions or concerns regarding the Act and may be the same person as the Responsible Authority.

The Data Practices Compliance Official is:

Marla Oakland
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 individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable. Summary data is public data unless otherwise classified by state or federal law or temporary classification.

Public Data Access Policy

Pursuant to Minnesota Statutes § 13.025 and 13.03, the City of Bloomington has established this **Public Data Access Policy**.

Right to Access Public Data

All Government Data, 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 A](#). Members of the public may inspect the data before deciding to request copies.

How to Make a Data Request

The City requires members of the public to submit a written request for access to government data. To submit a request, a member of the public should use the City's online request process on the [Data Practices](#) webpage. Alternative options include email, fax, mail, or in person.

If a member of the public chooses an alternative option, the request must include:

- A clear statement that a data request is being made pursuant to the Minnesota Government Data Practices Act.
- Whether the requestor wishes to inspect the data, receive copies, or both.
- A clear description of the data that is being requested.

The City cannot require a member of the public to provide identifying information or explain the reason for the data request. However, City staff may ask for personal information if it is necessary for mailing the requested data (either by U.S. Mail or through electronic transmission).

If the City does not understand a requestor's data request and has no way to contact the requestor, the City will not be able to process the data request.

How the City Responds to a Data Request

Upon receiving a data request, the Responsible Authority, Data Practices Compliance Official, or Designee will review it, acknowledge such receipt, attempt to clarify anything unclear about the request, and, if applicable, provide notice about the costs of supplying data and the City's requirement to prepay.

- If the City does not have the data, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor as soon as reasonably possible.
- If the City has the data, but it 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 identify the law(s) that prevent the requestor from accessing 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 as 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 allow.
 - Response time may vary based on the scope, volume, and complexity, as well as the number of requests made by a requestor within a specific date range.
- When the public data is compiled and available for release, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor of its availability by either:
 - Providing an electronic download through the City's online data request portal.
 - Arranging a time, date, and place for the requestor to inspect the data, if they have requested an inspection.
 - Providing paper copies of the data as requested. The requestor may choose to pick up the copies, or the copies will be mailed to them.
 - The City will suspend responses to data requests if the requester does not inspect or collect the data within five business days.

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 the City for an explanation of the meaning of the 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.

The City is not required to respond to questions that are not about a member of the public's data requests or requests for government data.

Requests for Summary Data

Summary Data may be 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.

Upon receiving a request for summary data, the City will respond regarding any needed clarification, details of whether and when the City may prepare summary data, and a cost estimate if applicable.

Data Subjects Rights and Access Policy

Pursuant to Minnesota Statutes § 13.025 and 13.03, the City of Bloomington has established this **Data Subjects Rights and Access Policy**.

Data Subjects

In the normal course of business, the City collects, maintains, and disseminates Government Data 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 ensure 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.

Classification of Data About Data Subjects

Government data about an individual have one of three classifications. These classifications determine who is legally allowed to access the data. Data about the data subject are classified by state law as public, private, or confidential. Here are some definitions and examples for each classification:

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.

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.

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 [Appendix B: Classification of Data](#) for more information about the classifications.

Data Subjects' Rights and Access

Data subjects have the right to inspect, free of charge, public and private Government Data about themselves. 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 to request copies.

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) (under the age of 18). Legal guardians have this same right related to the minors for whom they are appointed as guardian.

Minors have the right to request the City not to give data about them to their parent or legal guardian, 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; see [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.

When the City Collects Data

When the City requests that a data subject provide data that are not public, the City must give the data subject 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 from a data subject before the City can use or release the data for any other purposes. This permission is called Informed Consent to Release; see [Appendix D](#) (or access the form [here](#)).

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.

Challenging the 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.

How to Make a Data Subject Request

The City requires members of the public to submit a written request for access to government data. To submit a request, a member of the public should use the City's online request process on the [Data Practices](#) webpage. Alternative options include email, fax, mail, or in person.

If a member of the public chooses an alternative option, the request must be submitted to the Responsible Authority or Designee and include:

- A clear statement that a data request is being made pursuant to the Minnesota Government Data Practices Act. If the request is to inspect the data, receive copies, or both.
- A clear description of the data that is being requested.
- Identifying information that proves a requestor is the data subject, or the data subject's parent/guardian (typically a copy of a government-issued ID).
- Completed Informed Consent to Release completed by the subject of the data.

The City cannot require a member of the public to provide identifying information or explain the reason for the data request. However, City staff may request proof of identity to verify that the requestor is the data subject and is eligible to access private or nonpublic data. If the requestor is seeking data about their minor child, they must provide proof of being the child's parent. A legal guardian must present legal documentation verifying their guardianship.

If the City does not understand a requestor's data request and has no way to contact a requestor, the City will not be able to process the data request.

How the City Responds to a Data Subject Request

Upon receiving a data request, the Responsible Authority, Data Practices Compliance Official, or Designee will review it, acknowledge such receipt, attempt to clarify anything unclear about the request, and, if applicable, provide notice about the costs of supplying data and the City's requirement to prepay.

- The City will confirm a requestor's identity as the data subject, parent, or legal guardian. This is called Standards for Verifying Identity; see [Appendix E](#).
- If the City does not have the data, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor within 10 business days.
- If the City has the data, but the data is confidential or not public about someone else, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor within 10 business days and identify the law(s) that prevent the City from releasing 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.
- When the data is compiled and available for release, the Responsible Authority, Data Practices Compliance Official, or Designee will notify the requestor of its availability by either:
 - Providing an electronic download through the City's online data request portal.

- Arranging a time, date, and place for the requestor to inspect the data, for free, if the requestor has requested an inspection.
- Providing paper copies of the data as requested. The requestor may choose to pick up the copies, or the copies will be mailed to them.

Once the City has provided access to the data requested, the City does not have to show the data subject the data again for six months unless there is a dispute or the City collects or creates new data about the data subject.

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 the City for an explanation of the meaning of the 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.

The City is not required to respond to questions that are not about a data subject's data requests or requests for government data.

Policy for Ensuring the Security of Not Public Data

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.

Procedures for Implementing this Policy

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 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, 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.

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 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.

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.

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.

Appendix A: Copy Costs

When a fee is charged, members of the public are charged for the costs of searching for and retrieving the data and making copies or electronically sending the data. Data subjects are not charged for search and retrieval time.

Data Format	Fee
Paper copies – 101 or more pages, black and white, letter or legal sized paper copies	\$35 per hour of staff time
Paper copies – fewer than 101 pages	No charge
Paper copies – color	\$.60 per page, plus \$35 per hour of staff time
Electronic copies – fewer than three hours of staff time	No charge
Electronic copies – three or more hours of staff time	\$35/hour

Appendix B: Classification of Data

The Act divides all government data into three broad classifications: 1) data on individuals, 2) data not on individuals, and 3) data on decedents. These classifications each have three subcategories that determine who can access the data. The following chart provides the framework for classification and access:

Data on Individuals	Data Not on Individuals	Data on Decedents	Who Has Access
Public	Public	Public	Anyone
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.

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 to deny
Name of minor (individual younger than 18 years)

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, accommodation will be provided to allow individuals with disabilities to participate in all City of Bloomington services, programs and activities.

Data and Records Division

1800 W. Old Shakopee Road
Bloomington, MN 55431-3027

PH 952-563-4738
MN Relay 711

[Email Us](#)
Updated: 02/2026

Appendix D: Informed Consent to Release



Informed Consent to Release

Notice: Under data privacy laws, certain information is classified as private and is available only to you, to City employees whose work assignments require access, and to entities or agencies authorized by statute to gain access to this information. Completion of this form will allow the person or entity listed below to information in the custody of the City of Bloomington that relates to you.

I, , authorize the City of Bloomington to release
and disclose to the following information:

I agree to hold harmless the City of Bloomington from any liability arising from the release of the information that is in accordance with this *Informed Consent to Release*.

I understand that I may cancel this *Informed Consent to Release* at any time prior to the release of information and that, in any event, this release expires automatically 90 days after the date of signing.

Signed this day of 20

Signature of individual authorizing release

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, accommodation will be provided to allow individuals with disabilities to participate in all City of Bloomington services, programs and activities. Upon request, this information can be available in braille, large print, audio tape/or computer disk.

Appendix E: Standards for Verifying Identity

The following constitute proof of identity. Proof of identity is required when a data subject (or parent/legal guardian) has submitted a request for private data

An adult individual must show a valid photo ID, such as

- a state driver's license
- a military ID
- a passport
- a Minnesota ID
- a Minnesota tribal ID

A minor individual must show a valid photo ID, such as

- a state driver's license
- a military ID
- a passport
- a Minnesota ID
- a Minnesota Tribal ID
- a Minnesota school ID

The parent or guardian of a minor must show a valid photo ID and either

- a certified copy of the minor's birth certificate or
- a certified copy of documents that establish the parent or guardian's relationship to the child, such as
 - a court order relating to divorce, separation, custody, foster care
 - a foster care contract
 - an affidavit of parentage

The legal guardian for an individual must show a valid photo ID and a certified copy of appropriate documentation of formal or informal appointment as guardian, such as

- court order(s)
- valid power of attorney