FREEBORN COUNTY
GUIDELINES AND PROCEDURES
FOR
MINNESOTA
GOVERNMENT DATA PRACTICES ACT

Adopted by the
Freeborn County Board of Commissioners
July 19, 2022

To the extent that the Minnesota Government Data Practices Act changes, these guidelines and procedures shall be construed as consistent with those changes.

FREEBORN COUNTY GUIDELINES AND PROCEDURES FOR MINNESOTA GOVERNMENT DATA PRACTICES ACT

Table of Contents

MINNESOTA GOVERNMENT DATA PRACTICES ACT

Introduction

These guidelines and procedures provide direction in complying with those portions of the MGDPA that relate to *public access to government data* and to the *rights of subjects of data*.

The public access requirements are:

- The presumption that all government data are public unless classified as not public by state or federal statute;
- The right of any person to know what kinds of data are collected by the government entity and how that data is classified;
- The right of any person to inspect, at no charge, all public government data at reasonable times and places;
- The right of any person to have public data explained in an understandable way;
- The right of any person to get copies of public government data at a reasonable cost;
- The right of any person to an appropriate and prompt response from the government entity when exercising these rights; and
- The right of any person to be informed of the authority by which an entity can deny access to government data.

A BRIEF OVERVIEW OF THE MINNESOTA GOVERNMENT DATA PRACTICES ACT

The Minnesota Government Data Practices Act regulates the management of all government data that are created, collected, received, or released by a government entity, no matter what form the data are in, or how they are stored or used.

Briefly, the Act regulates:

- what data can be collected;
- who may see or get copies of the data;
- the classification of specific types of government data;
- the duties of government personnel in administering the Act;
- procedures for access to the data;
- procedures for classifying data as not public;
- civil penalties for violation of the Act; and
- the charging of fees for copies of government data.

Government data is either *data on individuals or data not on individuals.* Data on individuals are classified as either public, private, or confidential. Data not on individuals are classified as public, nonpublic, or protected nonpublic. This classification system determines how government data are handled (see chart below).

Data on Individuals	**Meaning of Classification**	**Data *Not* on Individuals**
Public	Available to anyone for any reason	Public
Private	Available only to the data subject and to anyone authorized by the data subject or by law to see it	Nonpublic
Confidential	Not available to the public or the data subject	Protected Nonpublic

I. COLLECTION OF GOVERNMENT DATA

What is the Minnesota Government Data Practices Act?

The Minnesota Government Data Practices Act (MGDPA), which is Chapter 13 of Minnesota Statutes, is a state law that controls how government data are collected, created, stored, maintained, used, and disseminated.

What are Government Data?

Government data are all data maintained in any recorded form by government entities, including counties. As long as data are recorded in some way by a government entity, they are government data, no matter what physical form they are in, or how they are stored or used. Government data may be stored on paper forms/records/files, in electronic form, on audio or video tape, on charts, maps, etc. Government data normally do not include mental impressions.

Persons or entities licensed or funded by, or under contract to, a government entity are subject to the MGDPA to the extent specified in the licensing, contract, or funding agreement.

Official records must be kept Minn. Stat. § 15.17, subd. 1 requires all officers and agencies of the state, and all officers and agencies of the counties, cities, and towns to make and keep all records necessary for a full and accurate knowledge of their official activities. Requirements for collecting, creating, maintaining, storing, and disseminating data are found in Minn. Stat. Ch. 13 and Minn. R. 1205, the Minnesota Government Data Practices Act and Rules.

A. EXTENT - The collection and storage of public, private, and confidential data on individuals are limited to that necessary for the administration and management of programs specifically authorized or mandated by the state, local governing body, or the federal government.

B. DEFINITIONS

1. **Data Inventory** - The public document required by Minn. Stat. § 13.025, subd. 1, containing the name of the responsible authority and the individual designee, title and address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the government entity. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory.

2. **Authorized Representative** – The Individual, entity, or person authorized to act on behalf of another individual, entity or person. For the purposes

of the Act, the authorized representative may include, but is not limited to: (a) in the case of a minor, a parent, or guardian, (see Section IX.B, Notification to Minors); (b) an attorney acting on behalf of an individual when the individual has given written informed consent; (c) any other individual entity, or person given written authorization by the data subject; or (d) an insurer or its representative, provided that the data subject has given informed consent for the release of the information, (e) court appointed guardian/conservator.

3. **Court Order** - The direction of a judge, or other appropriate presiding judicial officer made or entered in writing, or on the record in a legal proceeding.

4. **Data** - All data collected, created, received, maintained, or disseminated by a government entity regardless of its physical form, storage media, or conditions of use, including, but not limited to, paper records and files, microfilm, computer media, or other processes.

5. **Data Subject** - The individual or person about whom the data is created or collected.

6. **Designee** - Any person designated by a responsible authority (a) to be in charge of individual files or systems containing government data and (b) to receive and comply with requests for government data.

7. **Government Entity** – A state agency, statewide system, or political subdivision.

8. **Individual** - A natural person. In the case of a minor or an individual adjudged mentally incompetent, “individual” includes a parent or guardian or an individual acting as a parent or guardian in the absence of a parent or guardian, except that the responsible authority shall withhold data from parents or guardians or individuals acting as parents or guardians in the absence of parents or guardians, upon request by the minor if the responsible authority determines that withholding the data would be in the best interest of the minor.

9. **Informed Consent** - The written consent that must be given by a data subject to allow disclosure of private data about the individual.

10. **Person** - Any individual, partnership, corporation, association, business trust, or legal representative of an organization.

11. **Political Subdivision** - Any county, statutory or home rule charter city, school district, special district, any town exercising powers under Minn. Stat. 368 and located in a metropolitan area, and any board, commission,

district or authority created pursuant to law, local ordinance, or charter provision. It includes any nonprofit corporation which is a community action agency organized to qualify for public funds, or any nonprofit social service agency which performs services under contract to a government entity to the extent that the nonprofit social service individuals because of a contractual relationship with a government entity.

12. **Representative of the Decedent** - The personal representative of the estate of the decedent during the period of administration, or if no personal representative has been appointed, or after discharge, the surviving spouse, any child of the decedent, or, if there are no surviving spouse or children, the parents of the decedent.

13. **Requestor** - The individual, entity, or person requesting access and/or copies of the government data.

14. **Responsible Authority - Counties** - Each elected official of the county shall be the responsible authority of the respective office. An individual who is an employee of the county shall be appointed by the County Board to be the responsible authority for any data administered outside the departments of elected officials. For a statewide system, the responsible authority is the commissioner of any state department, or any executive officer designated by statute or executive order as responsible for such system.

15. **Rules –** "The Rules Governing the Enforcement of the Minnesota Government Data Practices Act. "Minn. R. Chap. 1205.

16. **State Agency** – The state, the University of Minnesota, and any office, officer, department division, bureau, board, commission, authority, district, or agency of the state.

17. **Statewide System** – Any recordkeeping system in which government data is collected, stored, disseminated, and used by means of a system common to one or more state agencies or more than one of its political subdivisions or any combination of state agencies and political subdivisions.

18. **Temporary Classification** - An application by a state agency, statewide system, or political subdivision, pursuant to Minn. Stat. § 13.06 which has been approved by the Commissioner of Administration to classify government data not classified by state statute or federal law as either private or confidential for data on individuals, or nonpublic or protected nonpublic for data not on individuals.

19. **Tennessen Warning** - Those rights, communicated to an individual asked to supply private or confidential data concerning himself or herself.

II. CLASSIFICATION OF GOVERNMENT DATA

For the purposes of these guidelines, government data is divided into four types; (a) data on individuals, which is classified as either public, private, or confidential; (b) data not on individuals, which is classified as either public, nonpublic, or protected nonpublic; (c) statistical or summary data derived from data on individuals in which individuals are not identified; and (d) data on decedents. These classifications, the criteria for classification, and the description of who has access are as follows:

A. DATA ON INDIVIDUALS

1. Public Data on Individuals

a. **Definition:** All data on individuals is public, unless classified as private or confidential.

b. **Data on Individuals is Public if:**

1) A statute or federal law requires or allows the collection of the data and does not classify the data as private or confidential.

2) An application for Temporary Classification for private or confidential data on individuals is disapproved by the commissioner of Administration.

3) The data is summary or statistical data derived from data on individuals.

4) Private or confidential data becomes public in order to comply with either judicial or administrative rules pertaining to the conduct of legal action. (For example: Private or confidential data which is presented in court and made public by the court.

c. **Access:** All public data on individuals is accessible by any person regardless of their interest in that data.

2. Private Data on Individuals

a. Definition: Private data on individuals is data which is not accessible to the public, but is accessible to the individual subject of the data.

b. Tennessen Warning: Except for law enforcement investigations, a Tennessen Warning must be given when private data is collected from the subject of the data (Section IX.A describes the Tennessen Warning.)

A Tennessen Warning need not be given when private data is collected from someone other than the subject of the data.

c. Data on Individuals is Private if:

1) A state statute or federal law expressly classifies the data as not accessible to the public, but accessible to the subject of the data.

2) A temporary Classification of private has been approved by the Commissioner of Administration and has not expired.

3) If data is classified as both private and confidential by state or federal law, the data is private.

d. **Access:** Private data on individuals is accessible to:

1) The individual subject of the data or the representative as authorized in writing (if the subject is a minor, usually by the subject's parent or guardian).

2) Individuals, entities, or persons who have been given express written permission by the data subject.

3) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.

4) Individuals, entities, or persons who used, stored, and disseminated government data collected prior to August 1, 1975, with the condition that use, storage, and dissemination was not accessible to the public, but accessible to the data subject. Use, storage, and dissemination of this data is limited to the purposes for which it was originally collected.

5) Individuals, entities, or persons for which a state, local, or federal law authorizes new use or new dissemination of the data.

6) Individuals, entities, or persons subsequent to the collection of the data and subsequent to the communication of the Tennessen Warning, when specifically approved by the Commissioner of Administration, as necessary, to carry out a function assigned by law.

7) Pursuant to court order.

8) Individuals, entities, or persons as otherwise provided by law.

3. **Confidential Data on Individuals**

a. **Definition:** Data on individuals is confidential if it is made by statute or federal law not accessible by the public and not accessible to the individual subject of the data.

b. **Tennessen Warning:** Except for law enforcement investigations, a Tennessen Warning must be given when confidential data is collected from the subject of the data.

A Tennessen Warning is not given when confidential data is collected from someone other than the subject of the data.

c. **Data on Individuals is Confidential if:**

1) A state or federal statute expressly provides that: (a) the data shall not be available to either the public or

to the data subject, or (b) the data shall not be available to anyone except those agencies which need the data for agency purposes.

2) A Temporary Classification of confidential has been approved by the Commissioner of Administration and has not expired.

d. **Access:**

1) Individuals, entities, or persons who are authorized by state, local, or federal law to gain access.

2) Personnel within the entity whose work assignment requires access as determined by the responsible authority, or the designee.

3) Individuals, entities, or persons who used, stored, and disseminated government data collected prior to August 1, 1975, with the condition that the data was not accessible to the individual subject of the data.

4) Individuals, entities, or persons for which a state or federal law authorizes a new use or new dissemination of the data.

5) Individuals, entities, or persons subsequent to the collection of the data and subsequent to the communication of the Tennessen Warning, when specifically approved by the Commissioner of Administration, as necessary, to carry out a function assigned by law.

6) Pursuant to court order.

7) Individuals, entities, or persons as otherwise provided by law.

B. PUBLIC, NONPUBLIC, OR PROTECTED NONPUBLIC DATA NOT ON INDIVIDUALS.

1. **Public Data Not on Individuals**

    a. **Definition:** Public data not on individuals means data not on individuals which is accessible to the public.

    b. **Data Not on Individuals is Public if:**

        1) A statute or federal law does not expressly classify the data as not public.

        2) An application for Temporary Classification for data as nonpublic or protected nonpublic is not approved by the Commissioner of Administration.

        3) A statute required the data to be made available to the public.

    c. **Access:** Public data not on individuals is accessible to any person regardless of their interest in the data.

2. **Nonpublic Data Not on Individuals**

    a. **Definition:** 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 a "Person" as defined in Section I.B., paragraph 10.

    b. **Data Not on Individuals is Nonpublic if:**

        1) A state statute or federal law classifies the data as not public, but accessible to the subject of the data, if any.

        2) A temporary Classification of data as nonpublic has been approved by the Commissioner of Administration.

    c. **Access:** Nonpublic data not on individuals is accessible to:

        1) The subject of the data, if any.

2) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.

3) Individuals, entities, or persons authorized by statute or federal statute to gain access.

4) It is reasonable to conclude that access to the data should be limited to entities or persons who have the legal authority to do so, and to entity staff on a need-to-know basis, that a representative of the organization which is the subject to the data may access the nonpublic data and may consent to its release.

5) Pursuant to court order.

6) Individuals, entities, or persons as otherwise provided by law.

3. **Protected Nonpublic Data Not on Individuals**

a. **Definition:** Protected nonpublic data not on individuals means data which is not public and not accessible to the subject of the data, if any. As used here, the subject data means a “Person” as defined in Section 1.B., paragraph 10.

b. **Data Not on Individuals is Protected Nonpublic if:**

1) A state statute or federal law classifies the data as not accessible to the public and not accessible to the data subject.

2) A Temporary Classification of government data as protected nonpublic has been approved by the Commissioner of Administration.

c. **Access:** Protected nonpublic data not on individuals is accessible to:

1) Personnel within the entity whose work assignment requires access as determined by the responsible authority or the designee.

2) Individuals, entities, or persons authorized by statute or federal law to gain access.

3) Pursuant to a court order.

4) Individuals, entities, or persons as otherwise provided by law.

C. SUMMARY DATA

1. **Definition:** Summary data means statistical records and reports derived from data on individuals, but in which the individuals are not identified and neither their identities nor other characteristics that could uniquely identify the individual is ascertainable.

2. **Data is Summary Data if:**

    a. All data elements that could link the data to a specific individual have been removed; AND,

    b. Any list of numbers or other data which could uniquely identify an individual is separated from the summary data and is not available to persons who gain access to or possess summary data.

3. **Access:** Unless classified by a Temporary Classification, summary data is public and may be requested by and made available to any individual or person, including a governmental entity.

D. DATA ON DECEDENTS

1. **Private Data on Decedents**

    a. **Definition.** Upon death, private and confidential data on an individual shall become, respectively, private data on decedents and confidential data on decedents.

b. **Access:**

1) Access is available to the personal representative of the estate during the administration or if no personal representative, the surviving spouse, any child of the decedent, or if no spouse or children, to the parent of the decedent.

2) A trustee appointed in a wrongful death action has access to appropriate private data on decedents concerning the data subject.

2. **Confidential Data on Decedents**

a. **Definition.** Confidential data on decedents means data which, prior to the death of the data subject, was classified by statute, federal law, or temporary classification as confidential data.

b. **Access.** Access to the data is the same as access to confidential data on individuals.

c. The representative of the decedent may exercise all rights which are conferred by the Act on individuals who are the subjects of confidential data, in the case of confidential data on decedents.

3. Release of private data on a decedent or confidential data on a decedent may also be obtained from a court following the procedure outlined in the statute. Any person may bring an action in the district court located in the county where the data is being maintained or, in the case of data maintained by state agency, in any county, to authorize release of private data on decedents or confidential data on decedents. The court must examine the data and consider whether the harm to the surviving spouse, children, or next-of-kin of the decedent, the harm to any other individual identified in the data, or the harm to the public outweighs the benefit to the person bringing the action or the benefit of the public.

4. Private data on decedents and confidential data on decedents shall become public when ten years have elapsed from the actual or presumed death of the individual and 30 years have elapsed from the creation of the data. For purposes of this determination, an individual is presumed to be dead if either 90 years elapsed since the creation of the data, or 90 years have elapsed since the individual's birth, whichever is earlier, except that an individual is not presumed to be dead if readily available data indicates that the individual is still living.

III. REQUEST FOR GOVERNMENT DATA

Refer to the Freeborn County Data Practices Policy for the Public Exhibit A (Appendix B), and/or Data Request by Subject of Data from Exhibit A (Appendix B) when copies are requested. No fee shall be charged for the actual costs of retrieving data or the viewing data.

A. REQUEST FOR DATA – GENERAL – Upon request to the responsible authority or designee, an authorized person shall be permitted to inspect government data at reasonable times and places, and if the party requests, they shall be informed of the meaning of the data. If the data requested is public data, no form is necessary. Upon request, public data may be disclosed over the telephone.

Regardless of where the data originates, if it is in your possession, it is government data and subject to the access provisions of the law.

The Public Data Request form or Request by Subject of Data form shall be completed for all requests by the public for government data which is classified as other than public

B. REQUESTES FOR DATA ON INDIVIDUALS BY THE DATA SUBJECT

1. Upon request and when access or copies are authorized, the designee shall provide copies of the private or public data on an individual to the subject of the data or authorized representative. See Minn. R. 1205.0500 if data subject is a minor.

2. The designee shall comply immediately, if reasonably possible, or within ten (10) working days of the date of request, if immediate compliance is not reasonably possible.

3. After an individual has been shown the private data and informed of its meaning, the data need not be disclosed to that individual for six (6) months, unless a dispute or action is pending (concerning accuracy of data), or additional information has been obtained on that individual.

C. REQUEST FOR SUMMARY DATA

1. Unless classified by a Temporary Classification, summary data derived from private or confidential data on individuals is public and the responsible authority or designee shall provide the summary data upon the written request for any individual or person.

2. Within ten (10) days of receipt of such request, the responsible authority or designee shall inform the requestor of the costs of preparing the summary data, if any.

3. The responsible authority or the designee shall:

    a. Provide the summary data requested **OR**

    b. Provide a written statement to the requestor describing a time schedule for preparing the requested data, including reasons for any delays; **OR**

    c. Provide access to the requestor to the private or confidential data so that the requestor can compile the summary data. Such access will be provided only when the requestor signs a non-disclosure agreement (see page 31); **OR**

    d. Provide a written statement to the requestor stating reasons why the requestor's access would compromise the private or confidential data.

4. A non-disclosure agreement is used to protect the confidentiality of government data when the requestor of the summary data prepares the summary by accessing private or confidential data on individuals.

    A non-disclosure agreement shall contain at least the following:

a. A general description of the private or confidential data which is being used to prepare summary data.

b. The purpose for which the summary data is being prepared.

c. A statement that the requestor understands that the requestor may be subject to the civil or criminal penalty provisions of the Act.

d. The signature of the requestor and the responsible authority, designee, or representative.

D. REQUESTS FOR GOVERNMENT DATA BY OTHER GOVERNMENT AGENCIES.

1. A responsible authority shall allow another responsible authority access to data classified as private, confidential, nonpublic, or protected nonpublic, or protected nonpublic only when the access is authorized or required by state or federal statute.

2. An agency that supplies government data under this section may require the requesting agency to pay the actual cost of supplying the data when the requested data is not provided in the normal course of business and not required by state or federal statute.

3. In most cases, data shall have the same classification in the hands of the agency receiving it as it had in the agency providing it, unless the classification is required to change to meet judicial or administrative requirements. When practical and necessary, the agency providing the requested information shall indicate the classification of the information.

4. When practical and necessary, the requesting agency not listed on the Tennessen Warning shall obtain the informed consent from the data subject(s) for information classified as private or confidential.

E. HOW DATA PRACTICES APPLIES TO CONTRACTRUAL LICENSING AND FUNDING RELATIONSHIP WITH GOVERNMENT ENTITIES.

1. Pursuant to Minn. Stat. § 13.05, subd. 6, if a person received public data on individuals from a government entity because that person has a

contract with that entity, the person must administer the data in a manner that is consistent with the MGDPA.

2. Pursuant to Minn. Stat. § 13.02, subd. 11, if a private person collects, receives, stores, uses, maintains or disseminates data because the person has a contract with a government entity to perform any of the entity's functions, all of the data are subject to the requirements. The contractor may be sued under Sec. 13.08, civil remedies. The contract must clearly inform the contractor of these responsibilities.

3. Pursuant to Minn. Stat. § 13.02, subd. 11, if the data is collected by a nonprofit social services entity which performs services under contract to a government entity, and the data is collected and used because of that contract, access to the data is regulated by the MGDPA.

4. If a third party is licensed by a government entity and the licensure is conditioned upon compliance with the MGDPA, or if the party has another type of contract with a government entity, the party is subject to the MGDPA to the extent specified in the contract or the licensing agreement.

IV. DATA REQUEST FORM AND DATA REQUEST FORM FOR SUBJECT OF DATA

A. DATA REQUEST FORM AND DATA REQUEST FORM FOR SUBJECT OF DATA. These forms provide a record of the requestor identification information and the government data requested, as well as the action taken by the responsible authority, or the designee, and any financial transaction which occurs.

B. WHEN COMPLETED. The Data Request form or Data Request form for Subject of Data should be completed for all requests by the public for government data classified as private, confidential, nonpublic, and protected nonpublic and for all requests by other government agencies for which the not public data is not routinely shared or provided in the normal course of business.

V. FEES FOR COPIES OF GOVERNMENT DATA

Pursuant to the Minnesota Government Data Practices Act and Freeborn County Board resolution and unless otherwise provided for by federal law, state statute or rule, fees for copies of government data shall be determined by departments based

on the costs of providing such services as set forth in Exhibit C. Fees shall be reasonable and consistent. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

NOTE: FEES SHALL NOT BE CHARGED TO THOSE INDIVIDUALS WHO ONLY WISH TO VIEW DATA.

NOTE: FEES MAY NOT BE CHARGED FOR SEPARATING PUBLIC FROM NONPUBLIC DATA.

A. COPIES PROVIDED AT NO CHARGE. When access is authorized, copies may be provided at no charge:

1. When another government agency or responsible authority requires or requests the record/document copies as part of the administration and management of an authorized program and the copies are usually provided as part of the normal course of business.

2. When records, documents, brochures, pamphlets, books, reports, or other similar publications are produced for free distribution to the public. A charge may be assessed if an individual request exceeds normal distribution.

3. When the court orders the requesting party to proceed in forma pauperis.

B. COPIES PROVIDED WITH CHARGE. When access is authorized, copies shall be provided at the applicable rate in the following circumstances:

1. Other government agencies are responsible authorities who require or request record documents or publication copies which are not usually provided or reproduced as part of the normal course of business.

2. Records, documents, brochures, pamphlets, books, reports, and other similar publications that are not normally provided or reproduced for distribution to the public.

3. Public data on individuals and public data <u>not</u> on individuals, particularly when the requestor is not the subject of the data.

C. COPYING FEES. Copying fees shall be charged in accordance with the Fee Schedule or those records, documents, and publications.

1. When copies are mailed, postage costs shall be added to the rates listed in Exhibit A (Appendix C), unless alternative arrangements have been made.

D. COLLECTION OF COPYING FEES. Fees shall be collected before releasing copies unless prior arrangements have been made.

E. FEE SCHEDULE. See Exhibit C.

F. DISPOSITION OF FEES. Copying fees collected shall be deposited in the appropriate account with the county treasurer.

VI. ASSIGNMENT OF DESIGNEE

The responsible authority may assign, in writing, one or more designees. The designee is the person in charge of individual files or systems containing government data and who receives and compiles with the requests for government data. Additionally, the designee shall implement the provisions of the Act, the rules, and these guidelines and procedures as directed by the responsible authority. All duties outlined as duties of the responsible authority may be delegated to the designee.

VII. DUTIES OF THE RESPONSIBLE AUTHORITY OR DESIGNEE.

A. DATA INVENTORY

1. The responsible authority shall prepare an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's government entity. Forms used to collect private and confidential data may be included in the inventory.

2. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory.

3. The responsible authority shall supply the document to the Commissioner of Administration, State of Minnesota, if requested by the Commissioner.

B. PROCEDURES FOR DISSEMINATION OF DATA.

1. The responsible authority shall ensure that each department establishes procedures to manage the dissemination of data. Collection, storage, use, and dissemination of private and confidential data shall be limited to what is necessary for the administration and management of programs authorized or mandated by the state, local governmental body, or the federal government.

2. Data cannot be collected, stored, used, or disseminated for any purpose other than the purpose stated to the individual when the data was originally collected unless:

    a. The data was collected prior to 1975, in which case the data can be used for the original purpose for which it was collected or for an additional purpose approved by the Commissioner of Administration.

    b. There is specific authorized for the use in state, local, or federal law.

    c. The additional use has been approved by the Commissioner of Administration, as necessary, to carry out a function designated by law.

    d. The individual data subject has given an informed consent for the additional use of the data.

C. DATA PROTECTION

The responsible authority shall establish procedures to assure that all data on individuals is accurate, complete, and current for the purpose for which it was collected, and establish appropriate security safeguards for all records containing data on individuals.

VIII. ACCESS TO GOVERNMENT DATA

A. WHO CAN MAKE A DATA REQUEST?

Anyone may exercise the right to access public government data by making a data request.

B. TO WHOM MUST A DATA REQUEST BE MADE?

1. A data request must be made to the responsible authority or to the appropriate designee(s).

2. The responsible authority for an entity must prepare summary data upon the request of any person if the request is in writing and the requestor pays for the cost to prepare the data.

3. The responsible authority may delegate the preparation of summary data to anyone outside of the entity, including the requestor, if

    a. That person's purpose is set forth in writing and the person agrees not to release any of the private or confidential data used to prepare the summary data; and

    b. If the entity reasonably determines that the access will not compromise private or confidential data on individuals.

4. The entity may require the requester to prepay the cost of preparing summary data.

IX. RIGHTS OF DATA SUBJECT

A. TENNESSEN WARNING – Rights of Subjects of Data.

1. Except for law enforcement investigations, every department that collects private and confidential data from an individual concerning that individual shall, prior to collecting the data, inform the individual of their rights as a subject of data. The notice must be given whenever:

    a. A government entity requests data;

    b. The data is requested from an individual;

    c. The data requested are private and confidential; **and**

    d. The data is about the individual from whom it is requested.

    All four of these conditions must be present before a Tennessen warning notice must be given. These rights are referred to as the Tennessen Warning.

A Tennessen Warning is not required when private and confidential data is collected from an individual who is not the subject of the data.

2. The Tennessen Warning consists of the following information that must be communicated to the individual from whom private or confidential data concerning the individual is collected.

    a. The purpose and intended use of the data. This is why the data are requested and how they will be used within the collecting entity.

    b. Whether the individual may refuse, or is legally required to supply the data. The subject has the right to know whether or not she/he is required by law to provide the data requested.

    c. Any consequences to the individual of either supplying or refusing to supply the data. The entity is required to state the consequences known to the entity at the time when the notice is given; and

    d. The identity of other persons or entities that are authorized by law to receive the data. The notice must specifically identify recipients that are known to the entity at the time the notice is given.

        NOTE: In accordance with the Federal Privacy Act of 1974, any federal, state, or local agency which requests an individual to disclose their social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

3. Tennessen Warning s may be either oral or written.

    a. An oral communication. This is not the preferred method of communicating the Tennessen Warning. However, it may be necessary under some circumstances. If an oral communication is necessary, the specific language communicated must be in written form and contained in the departmental data practices procedures and the situation documented.

    b. A written communication requiring the signature of the data subject (i.e., a signature attesting that the individual from whom private or confidential data is collected has read and understands their rights

pertaining to the requested data). The Tennessen Warning may be included on the form that collects the private or confidential data.

4. A sample format for the Notice of Rights Tennessen Warning is found on page 33.

B. NOTIFICATION TO MINORS

A minor has the right to request that the entity withhold private data about her/him from the parent or guardian. The entity may require that the request be in writing. A written request must include the reasons for withholding the data from the parents and must be signed by the minor.

Upon receipt of the request, the responsible authority must determine whether honoring the request is in the best interests of the minor. The responsible authority must consider, at a minimum:

1. Whether the minor is old and mature enough to explain the reasons for the request and to understand the consequences of making the request;

2. Whether denying access to the data may protect the minor from physical or emotional harm;

3. Whether there is a reason to believe that the minor's reasons for denying access to the parent(s) are reasonably accurate; and

4. Whether the nature of the data is such that disclosing the data to the parents could lead to physical or emotional harm to the minor. Minn. Rule 1205.0500 contains the procedures for the release of data about minors.

C. INFORMED CONSENT (see page 35)

1. Private data on individuals may be used by and disseminated to any individual or person by the responsible authority, or the designee, if the individual subject or subjects of the data have given their informed consent.

   NOTE: Informed consent cannot authorize a new purpose or a new use of <u>confidential</u> data on individuals.

2. Private data may be used by and disseminated to any entity (e.g., political subdivision, government agency, etc.) if the individual subject or subjects have given their informed consent.

3. All informed consents shall be in writing.

4. Informed consent shall not be deemed to have been given by an individual subject of the data by the signing of any statement authorizing any person or agency to disclose information about the individual to an insurer or its authorized representative, unless the statement is:

    a. In plain language;

    b. Dated;

    c. Specific in designating the particular persons or agencies the data subject is authorizing to disclose information about the data subject;

    d. Specific as to the nature of the information the subject is authorizing to be disclosed;

    e. Specific as to the persons or agencies to whom the subject is authorizing information to be disclosed;

    f. Specific s to the purpose or purposes for which the information may be used by any of the parties named in clause (e), both at the time of the disclosure and at any time in the future; and

    g. Specific as to its expiration date which should be within a reasonable period of time, not to exceed one year, except in the case of authorizations given in connection with applications for life insurance or noncancelable or guaranteed renewable health insurance and identified as such, two years after the date of the policy.

5. The informed consent for the disclosure of alcohol and drug abuse patient records may be made only if the consent is in writing and expressly states the fact that the request is for alcohol or drug abuse patient records. It should contain the following:

    a. The name of the program which is to make the disclosure;

    b. The name or title of the person or organization to which disclosure is to be made;

    c. The name of the patient;

d. The purpose or nature of information to be disclosed;

e. The extent or nature of information to be disclosed;

f. A statement that the consent is subject to revocation at any time, except to the extent that action has been taken in reliance thereon, and a specification of the data, event, or condition upon which it will expire without express revocation;

g. The date on which the consent is signed; and

h. The signature of the patient and, when required, of a person authorized to give consent.

6. A sample format is on page 35.

D. PROCEDURES FOR COMPLYING WITH DATA REQUESTS FROM AN INDIVDIUAL

The responsible authority shall ensure that each department establishes procedures to comply with requests for government data in an appropriate and prompt manner.

1. Upon request to the responsible authority, an individual shall be informed whether they are the subject of stored data on individuals, and whether it is classified as public, private, or confidential.

    a. The responsible authority shall provide access to the private or public data upon request by the individual subject of the data.

    b. An individual may contest the accuracy, current status, or completeness of public or private data. If the individual notifies the responsible authority in writing as to the nature of the disagreement with the data, the responsible authority shall, within 30 days, either correct the data and attempt to notify past recipients of inaccurate, incomplete, or out of date data, including recipients named by the individual, or notify the individual that the responsible authority believes the data to be correct. Subsequently, data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

2. The responsible authority shall prepare a public document, setting forth in writing the rights of the data subject and specific procedures in effect in the county for access by the data subject to public or private data on individuals.

    a. When a request is denied, the responsible authority must inform the requestor orally at the time of the request, and in writing, as soon thereafter as possible, and shall cite the statute, temporary classification, or federal law on which the determination is based.

    b. The responsible authority shall require the requestor to pay the actual costs of making and certifying copies of the data requested, except those exempted in Section V., subd. A. The requestor may not be charged for separating private or confidential data from public data.

    c. The responsible authority shall inform the requestor of the data's meaning, if asked to do so.

E. IF AN ENTITY DETERMINES THAT CHALLENGED DATA ARE ACCURATE AND/OR COMPLETE, AND THE DATA SUBJECT DISAGREES WITH THAT DETERMINATION, THE SUBJECT HAS THE RIGHT TO APPEAL THE ENTITY'S DETERMINATION TO THE COMMISSIONER OF ADMINISTRATION.

1. The subject has the right to take this set *only* after both the subject and the entity have properly completed all the steps in the data challenge process. The subject may appeal only the entity's determination about the accuracy and/or completeness of data.

2. The requirements for filing an appeal are set out at Minnesota Rules Section 1205.1600.

3. Procedure when data is not accurate or complete.

    a. An individual subject of the data may contest the accuracy or completeness of public or private data. To exercise the right, an individual shall notify, in writing, the responsible authority describing the nature of the disagreement. The responsible authority shall, within 30 days, 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. Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

4. The determination of the responsible authority may be appealed pursuant to the provisions of the Administrative Procedure Act., Minn. Stat. § 14.57 to 14.62 and Minn. R. 1205.1600, relating to contested cases. Upon receipt of an appeal by an individual by an individual, the commissioner of administration shall, before issuing the order and notice of a contested case hearing required by Chapter 14, try to resolve the dispute through education, conference, conciliation, or persuasion. If the parties consent, the commissioner may refer the matter to mediation. Following these efforts, the commissioner shall dismiss the appeal or issue the order and notice of hearing.

   a. Data on individuals that have been successfully challenged by an individual must be completed, corrected, or destroyed by a state government entity without regard to the requirements of Section 138.17.

   b. After completing, correcting, or destroying successfully challenged data, a state agency, political subdivision, or statewide system may retain a copy of the Commissioner of Administration's order issued under Chapter 14 or, if no order were issued, a summary of the dispute between the parties that does not contain any particulars of the successfully challenged data.

X. ROLE OF THE COMMISSIONER OF ADMINISTRATION.

A. Pursuant to Section 13.06, subdivision 6a, the Commissioner of the Minnesota Department of Administration is given the authority to approve new uses and disseminations of private and confidential data on individuals.

B. Section 13.05 of the Minnesota Government Data Practices Act (MGDPA) gives to the Commissioner certain powers with regard to approving temporary classifications of data.

C. Section 13.072 of the MGDPA, a government entity may be sued for violating any of the Act's provisions.

XI. CONSEQUENCES FOR NOT COMPLYING WITH THE MGDPA.

A. Pursuant to Section 13.08 of the MGDPA, a government entity may be sued for violating any of the Act's provisions.

B. Section 13.09 provides criminal penalties and disciplinary action as extreme as dismissal from public employment, for anyone who willfully (knowingly) violates a provision of the MGDPA.

XII. WHERE MORE INFORMATION CAN BE FOUND.

A. *Government entities must look to their legal advisor(s) for guidance and legal advice on data practices issues*. Only the legal advisor for an entity has the authority and responsibility to provide specific legal advice about the provisions of the MGDPA, and other laws, as they relate to that entity.

1. Minnesota Statutes Chapter 13 (the MGDPA) may be found on the website of the Minnesota Office of Revisor of Statutes. The Rules Governing Data Practices, promulgated by the Minnesota Department of Administration, also may be found at the website of the Office of Revisor of Statutes.

FREEBORN COUNTY

Non-Disclosure Agreement

1. General description of the private or confidential data which is being used to prepare summary data:

2. Purpose for which summary data is being prepared:

3. I,_____, representing _____

have requested the data described above and for the purposes stated and fully understand that I may be subject to the civil or criminal penalty provision of the Minnesota Data Practices Act in the event that the private or confidential data is disclosed.

> Min. Stat § 13.09. *Any person who willfully violates the provisions of Minnesota Statutes Chapter 13, or any rules adopted or regulation promulgated there under is guilty of a misdemeanor. Any willful violation of Minnesota by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.*

_____ _____

Requestor of Data Date

_____ _____

Responsible Authority/Designee Date

THE NOTICE OF RIGHTS TENNESSEN
WARNING INSTRUCTION GUIDE

Minnesota Statutes Section 13.04, subdivision 2

The notice must be given when:	1. An individual 2. Is asked to supply 3. Private or confidential data 4. Concerning self All four conditions must be present to trigger the notice requirement.
Statements must be included from the individual that inform the individual:	• Why the data is being collected and how the entity intends to use the data; • Whether the individual may refuse or is legally required to supply the data; • Any consequences to the individual of either supplying or refusing to supply the data; and • The identity of other persons or entities authorized by law to receive the data.
Consequences of giving the notice are:	Private or confidential data on individuals may be collected, stored, used, and released as described in the notice without liability to the entity.
Consequences on *not* giving the notice are:	Private or confidential data on individuals cannot be collected, stored, used, or released for any purposes other than those stated in the notice unless: • The individual subject of the data gives informed consent; • The Commissioner of Administration gives approval; or • A state or federal law subsequently authorizes or requires the new use or release.

“NOTICE OF RIGHTS”
SAMPLE FORMAT FOR TENNESSEN WARNING

In accordance with the Minnesota Government Data Practices Act, Freeborn County is required to inform you of your rights as they pertain to the private information collected from you. Your personal information we collect from you is private. Access to this information is available only to you and the agency collecting the information and other statutorily authorized agencies, unless you or a court authorize its release.

The Minnesota Government Data Practices Act requires that you be informed that the following information, which you are asked to provide, is considered private.

_____

The purpose and intended use of the requested information is:

_____

Furnishing the above information is voluntary, but refusal to supply the requested information will mean:

_____

_____
Name

_____
Date

Minn. Stat. § 13.04(2)

INFORMED CONSENT INSTRUCTION GUIDE

A. Enter the complete name and address of the entity that maintains the information. Include any relevant program names, staff names, titles and telephone numbers.

B. Identify, as specifically as possible, the reports, record names, or types of information or records that will be released.

C. Identify the entity or agencies to which the information will be released. Include the name and address of the entity. Include relevant staff names and titles. Be specific.

D. Describe specifically and completely the purpose(s) for seeking the client's informed consent and the new use(s) to which the information will be put.

E. Describe specifically and completely the known consequences of releasing the information.

F. Describe specifically and completely the known consequences of *not* releasing the information.

G. Instruct the person to sign the consent and enter the date on which the consent is signed.

H. As a general rule, a parent or guardian's signature should be obtained when the subject is under the age of 18 or has a legally appointed guardian; however, specific requirements for obtaining consent to release data in these circumstances vary. **Instructions for completing this portion of the form within our particular entity should be developed in consultation with the County Attorney's office.**

INFORMED CONSENT FOR THE RELEASE OF INFORMATION

I, _____
(Name of individual authorizing release)

authorize _____
(Name of individual, entity, or person holding record)

to disclose to _____
(Name of individual, entity, or person to receive the information)

the following information:

_____

for the purpose of:

_____

I understand that my records are protected under the state and/or federal privacy laws and cannot be disclosed without my written consent unless otherwise provided for by state or federal law. I understand that once this data is released that it may be subject to further disclosure without my written consent. I also understand that I may revoke this consent at any time except to the extent that action has been taken in reliance on it and that in any event, this consent at any time except to the extent that action has been taken in reliance on it and that in any event, this consent expires automatically in one year or as described below, whichever is earlier.

Specification of the date or condition upon which this consent expires:

_____

Executed this _____ day of _____, 20___.

_____
(Signature of individual authorizing release)

_____
Signature of parent, guardian, or authorized Representative, when required)

DATA PRACTICES NOTICE

I have been subpoenaed to testify before this court. I have been advised by the Office of the Freeborn County Attorney to provide the following information to the Court.

> "The data I have been requested to provide includes data which is classified as private data as defined by Minn. Statute Chapter 13, the Minnesota Government Data Practices Act. Pursuant to Minnesota Statute 13.03 and Minnesota Rule 1205.0100, Subp. 5, the Court's attention is called to this classification. The Data Practices Act requires that I may disclose this data only if the data subject has given written consent, a statute allows disclosure, or a court orders disclosure. If this court orders me to provide this private data, I will do so."

EXHIBIT A

Freeborn County Data Practices Policy For the Public Data Practices Contacts, Data Request Form and Copy Costs

Minnesota Statutes, sections 13.025 and 13.03 require this policy.

Adopted by the Freeborn County Board of Commissioners

July 19, 2022

Your Right to See Public Data

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 Freeborn County must keep all government data in a way that makes it easy for you to access public data. You have the right to look at (inspect), free of charge, all public data that we keep. You also have the right to get copies of public data. The Data Practices Act allows us to charge for copies. You have the right to look at data, free of charge, before deciding to request copies.

How to Request Public Data

You can ask to look at (inspect) data at our offices, or ask for copies of public data that we keep. Make a written request for the data to the appropriate person listed in the Data Practices Contacts document attached as Appendix A. You may make the written request for data by mail, email, or in person using the data request form attached as Appendix B.

If you do not use the data request form, your request should:

- Say that you are making a request for public data under the Government Data Practices Act (Minnesota Statutes, Chapter 13).
- Include whether you would like to inspect the data, have copies of the data, or both.
- Provide a clear description of the data you would like to inspect or have copied.

You are not required to identify yourself or explain the reason for your data request. However, you may need to provide us with some personal information for practical reasons (for example: if you want us to mail copies to you, you need to provide us with an address or P.O Box). If we do not understand your request and have no way to contact you, we cannot respond to your request.

How We Will Respond to Your Data Request

Upon receiving your request, we will review it.

- We may ask you to clarify what data you are requesting. If we do not have the data, we will notify you in writing as soon as reasonably possible.
- If we have the data, but we are not allowed to give it to you, we will tell you as soon as reasonably possible and identify the law that prevents us from providing the data.

- If we have the data, and the data are public, we will respond to your request appropriately and promptly, within a reasonable amount of time by doing one of the following:

    - Arrange a date, time, and place for you to inspect the data at our offices; or
    - You may choose to pick up your copies, or we will mail or email them to you. We will provide electronic copies (such as email or CD-ROM) upon request, if we keep the data in that format and we can reasonably make a copy. We will also arrange for you to pre-pay for the copies.
    - Response time may be impacted by the size and/or complexity of your request, and also by the number of requests you make in a given period of time.

Following our response, if you do not arrange within ten days to inspect the data or pay for the copies, we will conclude that you no longer want the data and will consider your request closed. If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please tell the person who provided the data to you. We will give you an explanation if you ask.

The Data Practices Act does not require us to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. For example, if the data you request are on paper only, we are not required to create electronic documents to respond to your request. If we agree to create data in response to your request, we will work with you on the details of your request, including cost and response time.

We are also not required to respond to questions that are not about your data requests, or requests for government data.

Requests for Summary Data

Summary data are statistical records or reports created by removing identifying information about individuals from entirely private or confidential data. The preparation of summary data is not a means to gain access to private or confidential data on individuals. Freeborn County will prepare summary data if you request it in writing and pre-pay for the cost of creating the data. Upon receiving your written request, we will respond within ten business days with the data or details on when the data will be ready and how much we will charge.

Standards for Verifying Identity

The following constitute proof of identity:

- An adult individual must provide a valid photo ID, such as
    - a driver's license
    - a state-issued ID

    - a tribal ID
    - a military ID
    - a passport
    - the foreign equivalent of any of the above

- A minor individual must provide a valid photo ID, such as
    - a driver's license
    - a state-issued ID (including a school/student ID)
    - a tribal ID
    - a military ID
    - a passport
    - the foreign equivalent of any of the above

- The parent or guardian of a minor must provide 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 provide 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

Note: Individuals who do not inspect data or pick up copies of data in person may be required to provide either notarized or certified copies of the documents that are required or an affidavit of ID.

Appendix A
Freeborn County Data Practices Contacts

The following table provides contact information for the individuals who are responsible for responding to requests for data. The "Responsible Authority" is the individual responsible for establishing and overseeing data access processes. The "Data Practices Compliance Official" is the individual whom questions about, or problems related to, data practices should be directed.

Office	**Responsible Authority, Data Practices Compliance Official and Designees: Freeborn County Administrator** PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5116; Fax: 507-377-5109
County Attorney	*Responsible Authority: David Walker, County Attorney* *Designee: Erin M. O'Brien, Assistant County Attorney* PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5192; Fax: 507-377-5196 Erin.Obrien@co.freeborn.mn.us
Sheriff	*Responsible Authority: Kurt Freitag, County Sheriff* *Designee: Paige Bangert, LEC Records Manager* PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5239, Fax: 507-377-5257 Paige.Bangert@co.freeborn.mn.us

All other County Offices	*Responsible Authority: Freeborn County Administrator* PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5116, Fax: 507-377-5109 Email: *Data Practice Compliance Official: Erin M. O'Brien* Erin.Obrien@co.freeborn.mn.us
	Designees: Assessor County Assessor PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5176, Fax: 507-377-5259 Email: Auditor/Treasurer Patricia Martinson, County Auditor-Treasurer PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5123; Fax: 507-377-5175 Patricia.Martinson@co.freeborn.mn.us Environmental Services Mark Goskeson, Environmental Services Director 2020 Pioneer Trail Albert Lea, MN 56007 (507) 377-5186; Fax: (507) 377-4688 Mark.Goskeson@co.freeborn.mn.us Highway Department/Public Works Phil Wacholz, County Engineer/Public Works Director 3300 Bridge Avenue Albert Lea, MN 56007 (507) 377-5188; Fax: (507) 377-5189 Philip.wacholz@co.freeborn.mn.us Human Services Suzi Nerison. Human Services Director PO Box 1246 203 Clark West Street Albert Lea, MN 56007 507-377-5401, Fax: 507-377-5498 Suzanne.Nerison@co.freeborn.mn.us

	Information Technology Scott Woitas, IT Director PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5102 Scott.Woitas@co.freeborn.mn.us Probation & Pre-Trial Services (*aka Court Services)* Lyndon Stinson, Director PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5137; Fax: 507-377-4695 Lyndon.Stinson@co.freeborn.mn.us Public Health Sue Yost, Public Health Director PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5100, Fax: 507-377-5272 Sue.Yost@co.freeborn.mn.us Recorder Kelly Hendrickson, Recorder/Registrar of Titles PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5791; Fax: 507-377-5265 Kelly.Hendrickson@co.freeborn.mn.us Veteran's Services Jeff Dahlen, Veteran's Services Officer PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5184; Fax 507-377-5256 Jeff.Dahlen@co.freeborn.mn.us

Appendix B
Freeborn County Data Request Form

Date of request: _____

I am requesting access to data in the following way:

☐ Inspection ☐ Copies ☐ Both Inspection and Copies

Note: Inspection is free, but there is a charge for copies. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

These are the data I am requesting:

_____

_____

_____

Note: Describe the data you are requesting as specifically as possible. If you need more space, please use the back of this form.

To request data as a data subject, you must show a valid state ID, such as a driver's license, military ID, or passport as proof of identity. To request data on behalf of the data subject, you must present proper written permission granting you such access.

Data Subject Name: _____

Address: _____

Phone Name: _____ Email: _____

Parent/Guardian Name (if applicable): _____

Signature of Data Subject or Parent/Guardian: _____

Freeborn County will respond to your request within 10 days.

(For office use)	
ID provided:	
Department name:	***Request handled by:***
Method of response:	
Charges:	
Amt Due:	***Received by:***
Notes	

Appendix C
Freeborn County Copy Costs – Members of the Public

Freeborn County, Minnesota Freeborn County charges members of the public for copies of government data. These charges are authorized under Minnesota Statutes, section 13.03, subdivision 3(c). You must pay for copies before we will give them to you. Except as noted below, we do not charge for copies if the cost is less than $5.00.

For 100 or Fewer Paper Copies – $0.25 Per Page

100 or fewer pages of black and white, letter or legal size paper copies cost $0.25 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 transmitting the data (e.g. sending the data by email).

In determining the actual cost of making copies, we factor in employee time, the cost of the materials onto which we are copying the data (paper, CD, DVD, etc.) and mailing costs (if any). If your request is for copies of data that we cannot reproduce ourselves, such as photographs, we will charge you the actual cost we must pay an outside vendor for the copies.

The cost of employee time to search for data, retrieve data, and make copies is $15.75 per hour. If, because of the subject matter of your request, we find it necessary for a higher-paid employee to search for and retrieve the data, we will calculate the search and retrieval portion of the copy charge at the higher salary/wage.

Assessor's Office:

Charge for copies as other departments; however,
"Freeborn County Online Mapping Service" is available.

Remote access fees:	$10.00 for daily fee; $250.00 for annual subscription

Electronic File of Property Tax/Real Estate Data:

Recorder's Office:

Copies of documents	$1.00 per page ($2.00 minimum) Mail request and response
Copies of documents	$0.25 per page (in person)
Copies from microfilm	$0.50 per page (in person, limited employee assistance)

Vital Records	(Minnesota Statutes, Section 144.226)	
	Certified Copies:	Non-certified copies:
Birth Certificate	$26.00	$13.00
Death Certificate	$13.00	$13.00
Marriage Certificate	$9.00	$9.00

Sheriff's Office Records Fee Schedule:

Police reports:	$0.25 per page
CD copy of photos:	$5.00 per CD
Scanned/printed photos	$1.00 per page
Copy of crash report:	$3.00 (Minnesota Statutes, Section 169.09, Subd. 13)

EXHIBIT B

Freeborn County Data Practices Policy:

Requests for Data About You and Your Rights as a Data Subject

Adopted by the Freeborn County Board of Commissioners

July 19, 2022

Policy and procedures required by Minnesota Statutes, section 13.025 and 13.03

What is a “Data Subject”?

When government has information recorded in any form (paper, harddrive, voicemail, video, email, etc.), that information is called “government data” under the Government Data Practices Act (Minnesota Statutes, Chapter 13). When we can identify you in government data, you are the “data subject” of that data. The Data Practices Act gives you, as a data subject, certain rights. This policy explains your rights as a data subject, and tells you how to request data about you, your minor child, or someone for whom you are the legal guardian.

When Freeborn County Has Data About You

Freeborn County has data on many people, such as if you are an employee of a government entity, the fact that you work there, and your job title and bargaining unit are public. We can collect and keep data about you only when we have a legal purpose to have the data. Admin must also keep all government data in a way that makes it easy for you to access data about you.

Government data about an individual have one of three “classifications.” These classifications determine who is legally allowed to see the data. Data about you are classified by state law as public, private, or confidential. Here are some examples:

Public Data

The Data Practices Act presumes that all government data are public unless a state or federal law says that the data are not public. We must give public data to anyone who asks. It does not matter who is asking for the data or why the person wants the data. The following are examples of public data about you that we might have: your name on an application for a Freeborn County program.

Private Data

We cannot give private data to the general public. We can share your private data with you, with someone who has your permission, with our government entity staff whose job requires or permits them to see the data, and with others as permitted by law or court order. The following are examples of private data about you that we might have: your Social Security Number.

Confidential Data

Confidential data have the most protection. Neither the public nor you can access confidential data even when the confidential data are about you. We can share confidential data about you with our government entity staff who have a work assignment to see the data, and to others as permitted by law or court order. The following is an example of confidential data about you: your identity as a mandated reporter of child abuse or neglect.

As a data subject, you have the following rights.

Access to Your Data

You have the right to look at (inspect), free of charge, public and private data that we keep about you. You also have the right to get copies of public and private data about you. The Data Practices Act allows us to charge for copies. You have the right to look at data, free of charge, before deciding to request copies.

Also, if you ask, we will tell you whether we keep data about you and whether the data are public, private, or confidential.

As a parent, you have the right to look at and get copies of public and private data about your minor children (under the age of 18). As a legally appointed guardian, you have the right to look at and get copies of public and private data about an individual for whom you are appointed guardian.

Minors have the right to ask us not to give data about them to their parent or guardian. If you are a minor, we will tell you that you have this right. We will ask you to put your request in writing and to include the reasons that we should deny your parents access to the data. We will make the final decision about your request based on your best interests.

When We Collect Data from You

When we ask you to provide data about yourself that are not public, we must give you a notice called a Tennessen warning. The notice controls what we do with the data that we collect from you. Usually, we can use and release the data only in the ways described in the notice.

We will ask for your written permission if we need to use or release private data about you in a different way, or if you ask us to release the data to another person. This permission is called informed consent.

Protecting Your Data

The Data Practices Act requires us to protect your data. We have established appropriate safeguards to ensure that your data are safe.

In the unfortunate event that we determine a security breach has occurred and an unauthorized person has gained access to your data, we will notify you as required by law.

When your Data are Inaccurate or Incomplete
You have the right to challenge the accuracy and/or completeness of public and private data about you. You also have the right to appeal our decision. If you are a minor, your parent or guardian has the right to challenge data about you.

How to Make a Request for Your Data

You can ask to look at (inspect) data at our offices by making a written request. You may also make a written request for or ask for copies of data that we have about you, your minor child, or an individual for whom you have been appointed legal guardian. Make the request to the office and person found on attached Appendix A. Use the data request form attached here as Appendix B.

Your request should:

- Say that you are making a request as a data subject, for data about you (or your child, or person for whom you are the legal guardian), under the Government Data Practices Act (Minnesota Statutes, Chapter 13).
- Include whether you would like to inspect the data, have copies of the data, or both.
- Provide a clear description of the data you would like to inspect or have copied.
- Provide proof that you are the data subject or data subject's parent/legal guardian.

We require proof of your identity before we can respond to your request for data. If you are requesting data about your minor child, you must show proof that you are the minor's parent. If you are a legal guardian, you must show legal documentation of your guardianship. If you do not provide proof that you are the data subject, we cannot respond to your request.

How We Respond to a Data Request

Upon receiving your request, we will review it.

- We may ask you to clarify what data you are requesting.
- We will ask you to confirm your identity as the data subject.
- If we have the data, but the data are confidential or not public data about someone else, we will notify you within 10 business days and identify the law that prevents us from providing the data. If we do not have the data, we will notify you as soon as reasonably possible.
- If we have the data, and the data are public or private data about you, we will respond to your request within 10 business days by doing one of the following:
    - Arrange a date, time, and place to inspect data in our offices, for free, or
    - Provide you with the data within 10 business days. You may choose to pick up your copies, or we will mail or fax them to you. We will provide electronic copies (such as email or CD-ROM) upon request if we keep the data in

electronic format. Information about copy charges is in Appendix C. We will arrange for you to pre-pay for the copies. Following our response, if you do not arrange within ten business days to inspect the data or pay for the copies, we will conclude that you no longer want the data and will consider your request closed.

- After we have provided you with your requested data, we do not have to show you the same data again for 6 months unless there is a dispute about the data or we collect or create new data about you.

If you do not understand some of the data (technical terminology, abbreviations, or acronyms), please tell the person who provided the data to you. We will give you an explanation if you ask.

The Data Practices Act does not require us to create or collect new data in response to a data request, or to provide data in a specific form or arrangement if we do not keep the data in that form or arrangement. For example, if the data you request are on paper only, we are not required to create electronic documents to respond to your request. If we agree to create data in response to your request, we will work with you on the details of your request, including cost and response time.

In addition, we are not required to respond to questions that are not about your data requests, or that are not requests for government data.

Requests for Summary Data

Summary Data are statistical records or reports that are prepared by removing all identifiers from private or confidential data on individuals. The preparation of summary data is not a means to gain access to private or confidential data. Freeborn County will prepare summary data if you make your request in writing and pre-pay for the cost of creating the data. Upon receiving your written request, we will respond within ten business days with the data or details of when the data will be ready and how much we will charge.

Standards for Verifying Identity

The following constitute proof of identity:

- An adult individual must provide a valid photo ID, such as
  - a driver's license
  - a state-issued ID
  - a tribal ID
  - a military ID
  - a passport
  - the foreign equivalent of any of the above
- A minor individual must provide a valid photo ID, such as

    - a driver's license
    - a state-issued ID (including a school/student ID)
    - a tribal ID
    - a military ID
    - a passport
    - the foreign equivalent of any of the above
- The parent or guardian of a minor must provide 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 provide 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

Note: Individuals who do not inspect data or pick up copies of data in person may be required to provide either notarized or certified copies of the documents that are required or an affidavit of ID.

Appendix A
Freeborn County Data Practices Contacts

The following table provides contact information for the individuals who are responsible for responding to requests for data. The "Responsible Authority" is the individual responsible for establishing and overseeing data access processes. The "Data Practices Compliance Official" is the individual whom questions about, or problems related to, data practices should be directed.

Office	**Responsible Authority, Data Practices Compliance Official and Designees: Freeborn County Administrator** PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5116; Fax: 507-377-5109 Email:
County Attorney	*Responsible Authority: David Walker, County Attorney* *Designee: Erin M. O'Brien, Assistant County Attorney* PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5192; Fax: 507-377-5196 Erin.Obrien@co.freeborn.mn.us
Sheriff	*Responsible Authority: Kurt Freitag, County Sheriff* *Designee: Paige Bangert, LEC Records Manager* PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5239, Fax: 507-377-5257 Paige.Bangert@co.freeborn.mn.us

All other County Offices	*Responsible Authority: Freeborn County Administrator* PO Box 1147, 411 S. Broadway, Albert Lea, MN 56007 507-377-5116, Fax: 507-377-5109 Email: *Data Practice Compliance Official: Erin M. O'Brien* Erin.Obrien@co.freeborn.mn.us
	Designees: Assessor County Assessor PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5176, Fax: 507-377-5259 Email: Auditor/Treasurer Patricia Martinson, County Auditor-Treasurer PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5123; Fax: 507-377-5175 Patricia.Martinson@co.freeborn.mn.us Environmental Services Mark Goskeson, Environmental Services Director 2020 Pioneer Trail Albert Lea, MN 56007 (507) 377-5186; Fax: (507) 377-4688 Mark.Goskeson@co.freeborn.mn.us Highway Department/Public Works Phil Wacholz, County Engineer/Public Works Director 3300 Bridge Avenue Albert Lea, MN 56007 (507) 377-5188; Fax: (507) 377-5189 Philip.wacholz@co.freeborn.mn.us Human Services Suzi Nerison. Human Services Director 203 Clark West Street, PO Box 1246 Albert Lea, MN 56007 507-377-5401, Fax: 507-377-5498 Suzanne.Nerison@co.freeborn.mn.us

	Information Technology Scott Woitas, IT Director PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5102 Scott.Woitas@co.freeborn.mn.us Probation & Pre-Trial Services (*aka Court Services)* Lyndon Stinson, Director PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5137; Fax: 507-377-4695 Lyndon.Stinson@co.freeborn.mn.us Public Health Sue Yost, Public Health Director PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5100, Fax: 507-377-5272 Sue.Yost@co.freeborn.mn.us Recorder Kelly Hendrickson PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5791; Fax: 507-377-5265 Kelly.Hendrickson@co.freeborn.mn.us Veteran's Services Jeff Dahlen, Veteran's Services Officer PO Box 1147, 411 S. Broadway Albert Lea, MN 56007 507-377-5184; Fax 507-377-5256 Jeff.Dahlen@co.freeborn.mn.us

Appendix B
Freeborn County Data Request Form

Date of request: _____

I am requesting access to data in the following way:

☐ Inspection ☐ Copies ☐ Both Inspection and Copies

Note: Inspection is free, but there is a charge for copies. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

These are the data I am requesting:

_____

_____

_____

Note: Describe the data you are requesting as specifically as possible. If you need more space, please use the back of this form.

To request data as a data subject, you must show a valid state ID, such as a driver's license, military ID, or passport as proof of identity. To request data on behalf of the data subject, you must present proper written permission granting you such access.

Data Subject Name: _____

Address: _____

Phone Name: _____ Email: _____

Parent/Guardian Name (if applicable): _____

Signature of Data Subject or Parent/Guardian: _____

Freeborn County will respond to your request within 10 days.

(For office use)	
ID provided:	
Department name:	***Request handled by:***
Method of response:	
Charges:	
Amt Due:	***Received by:***
Notes	

Appendix C
Freeborn County Copy Costs – Members of the Public

Freeborn County, Minnesota Freeborn County charges members of the public for copies of government data. These charges are authorized under Minnesota Statutes, section 13.03, subdivision 3(c).

You must pay for copies before we will give them to you. Except as noted below, we do not charge for copies if the cost is less than $5.00.

For 100 or Fewer Paper Copies – $.25 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 transmitting the data (e.g. sending the data by email).

In determining the actual cost of making copies, we factor in employee time, the cost of the materials onto which we are copying the data (paper, CD, DVD, etc.) and mailing costs (if any). If your request is for copies of data that we cannot reproduce ourselves, such as photographs, we will charge you the actual cost we must pay an outside vendor for the copies.

The cost of employee time to search for data, retrieve data, and make copies is $15.75 per hour. If, because of the subject matter of your request, we find it necessary for a higher-paid employee to search for and retrieve the data, we will calculate the search and retrieval portion of the copy charge at the higher salary/wage.

Assessor's Office:

Charge for copies as other departments; however,
"Freeborn County Online Mapping Service" is available.

Remote access fees:	$10.00 for daily fee;
	$250.00 for annual subscription

Electronic File of Property Tax/Real Estate Data:

Recorder's Office:

Copies of documents	$1.00 per page ($2.00 minimum) Mail request and response
Copies of documents	$0.25 per page (in person)
Copies from microfilm	$0.50 per page (in person, limited employee assistance)

Vital Records	(Minnesota Statutes, Section 144.226)	
	Certified Copies:	Non-certified copies:
Birth Certificate	$26.00	$13.00
Death Certificate	$13.00	$13.00
Marriage Certificate	$9.00	$9.00

Sheriff's Office Records Fee Schedule:

Police reports:	$0.25 per page
CD copy of photos:	$5.00 per CD
Scanned/printed photos	$1.00 per page
Copy of crash report:	$3.00 (Minnesota Statutes, Section 169.09, Subd. 13)

EXHIBIT C

FREEBORN COUNTY FEE SCHEDULE
EFFECTIVE SEPTEMBER 15,2020

County Wide Fees		
Copies of material related to a data request	Actual cost of producing documents per MN Stat. 13.03 Sub 3(c)	
Paper Copies- 100 or fewer pages	.25 per page one sided- .50 two sided	
Conference room	No Fee. Must be a government affiliated organization.	
All other media forms	Actual cost	

Probation		
Probation Supervision Fee (one time)	$200.00	
Diversion Program Fee	$150.00	
Pre-Trial Program Fee	$150.00	
Interstate/Intrastate Transfer Fee	$50.00	
Domestic Abuse Program Fee	$20 weekly	

Environmental Services		
Building Permits/Plan Review/State Surcharge	varies by project	there are fixed fees for certain projects and other projects go by valuation
Zoning Permit	$50.00	
Demo	$25.00	
Water Tests	depends on water test requested	most common at Bacteria/Nitrates $55.00 or Bacteria/Nitrates/Lead $75.00
Conditional Use Permit	$400.00	
Variance	$400.00	
Re-Zoning	$400.00	
Feedlot Permits	$100.00	0 - 299 animal units
	$200.00	300-999 animal units
	$300.00	1000 animal units and up
Rural Address	$100.00	
Septic	$100.00	
Plat Books	$40.00	
Small Business Recycling	$40.00	
Solid Waster/Hauler Permits	$50.00	$100 for new

Public Health		
Vaccine for Children Immunizations	$20.00	requested donation per each immunization
Un- and Under- Insured Adult Immunization	$20.00	requested donation per each immunization
Flu Vaccine and Administration	$40.00	
High Dose Flu Shot	$75.00	
Nurse Visit	$140.00	

Public Works		
Utility permit	$100.00	
Access permit	$100.00 / Residential *	$200.00 / Field Access *
Access permit - Commercial, Public Streets	$200.00	
Single Move/Single Trip Oversize/Overweight Permit Fee	$50.00	Applied to all Single Move/Single Trip Oversize/Overweight Permits
Axle fee for over design axle weight	$6.50/Over design axle weight (ODAW)/mile	ODAW = (actual axle weight/design axle weight)^4 (See ePermitting Website)
Right-of-Way Permit	$100.00/crossing *	
Mailbox	$115.50	Mailbox: $18.25 / Post: $97.25
Labor / Equipment Operator	Actual labor cost including wage plus benefits for employees including overtime when applicable.	
Single Axle Dump Truck	$50.00 / Hour	
Tandem Axle Dump Truck	$55.00 / Hour	
Maintainer/Motor Grader	$50.00 / Hour	
Wheel Loader	$50.00 / Hour	
Tracked Skid Loader	$45.00 / Hour	
Sweeper	$56.00 / Hour	2 Hour Minimum
Pickup - 1 Ton or Larger	$20.00 / Hour	
Pickup - 3/4 Ton or Smaller	$15.00 / Hour	
UTV	$30.00 / Hour	
Tractor - Under 100 hp	$30.00 / Hour	
Tractor - Over 100 hp	$40.00 / Hour	
Conference Room	No Fee. Must be a government affiliated organization.	
Park Reservations	No Fee	
Park Camping	No Fee. Permit required with prior approval plus proof of insurance.	Non Profit / Youth / Government only

* Fee waived at discretion of Public Works Director when mutally benefitting County.
Equipment rates do not include an operator.

FREEBORN COUNTY FEE SCHEDULE
EFFECTIVE SEPTEMBER 15,2020

Human Services		
Child Care Licensure (Initial)	$100.00	
Child Care Relicensure (every 2 years)	$65.00	
Detoxification Services / Fees	100% of the cost as billed by provider	
Out of Home Placement Fee (children)	Sliding fee based on income and as allowed per Statute	

SHERIFFS OFFICE/JAIL		
Booking Fee	$10 Per Day	
Cup/Spork/Sandal Fee	$7 Per Day	
Huber Fee	$30 Per Day	
Out of County Huber Fee	$30 Per Day	
Weekend Fee	$60.00	
PBT Fee	$5 per test	
Permit to carry a firearm	$100 new permit, $75 for renewal	Discounts may apply to Military and Law Enforcement personnel

CIVIL PROCESS FEES		
Service of summons, writs, subpoenas, or any process	$100.00	
Making a diligent search and inquiry and returning summons		
when defendant cannot be found	$100.00	
Returning executions unsatisfied when no money is collected	$100.00	
Posting three (3) notices	$100.00	
Conducting Mortgage Foreclosure/Execution Sales	$100.00	
Securing & safely keeping property in Replevin or attachment		
or on execution, per hour, per deputy	$100.00	
Service of Eviction Notice/Writ of Restitution per hour,		
per Deputy	$100.00	
Service of Order for Protection/Harassment Restraining		
Order	No Charge	
Redemption from Forclosure	$250.00	
Commission of execution after levy	5%	

RECORDS FEES		
reports- per page	$0.25	
Crash report	$3.00	
Photo Prints	$1.00	
Scanned Photes	$1.00	
vidoe/audio recording	$8.00	
Backgound- criminal local	$10.00	

RECORDERS FEES		
Fax/e-mail of Record	$10 plus copy fee	
Copies/Images of Record	$1/page	
Copies/Images of Recorded Mailed	$1/page ($2 min)	
Copies Reduced Plats/RLS/Half Sections/Parcel Maps	$3	
Uncertified Copies of Certificate of Title	$1/page ($10 max)	
Document Deposit (600.23)	$150/document/year	
Security Deposit (386.78)	$100 minimum	
Landshark Fees		
Credit Card Convience fee	$5 per transaction	
Set-up Fee	$50	
Monthly Fee	$50	
Document Image	$2	
Torrens Certificate	$2	
Ordination Recording	$50	

AUDITOR-TREASURER		
Auctioneer License	$20.00	
Auditor's Affidavit - Title 45	$50.00/hr	
Auditor's Certificate	$200.00	
Beer (3.2%) Off-Sale License	$75.00	
Beer (3.2%) On-Sale License	$100.00	
Beer (3.2%) on/Off Sale License	$150.00	

FREEBORN COUNTY FEE SCHEDULE
EFFECTIVE SEPTEMBER 15,2020

Dangerous Dog Registration	$200.00	
Delinquent Tax List	$50.00	
Escrow Tax File Processing/per file	$50.00	
Fireworks Display	$50.00	
Liquor License On-Sale	$2,000.00	
Sunday Liquor On-Sale	$240.00	
Tax Search - Certification/per parcel	$5.00	
Tax File Download	$50.00	
Tobacco Retailer License	$60.00	
Transient Merchant License	$150.00	
Certificate of Delinquent Tax	$10/parcel	
Wine License	$200.00	

LICENSE CENTER

Auto and Motorcycle Driver's Manual	$5.00	
CDL Truck Drivers Manual	$10.00	

ASSESSOR FEES-GIS / PROPERTY INFO DATA FEE SCHEDULE

Basic Bundle	$100.00	GIS Shapefiles Included: Parcel Boundaries & Road Centerlines
Enhanced Bundle	$500.00	GIS Shapefiles Includes Basic Bundle PLUS Townships, Sections,City Limits, Lot Lines, Parcel Lines, Road/Street, ROW and Water
IT Bundle	$1,500.00	Includes: Aerial Photos, Elevation Data, Parcel Boundaries, Road (purchaser to provide hard drive)
Building Data Speadsheet	$200.00	PIN, Style, Main year built, Main Area, TLA, Roll Type, Grade, Occupancy Code, Bedrooms and utilities
Ag Soils Land Data	$200.00	PIN, land type, Tillable CER, Acres per soil type, Symbol, Description, Total Acres, District, map area
Non-Ag Land Data	$200.00	PIN, Acres per land line, SF per land line, Total Acres, District, Map Area
3 year Sales Data	$200.00	PIN, Sale Date, Sale Amount, Seller, Buyer,NUTC Description, Adj. Sale Amount, District, Deed type,address
Tax and Assessment Speadsheet- AKA CDOWNO	$500.00	Payable year, Roll Type, PIN, MP, District, Town/city Code, School District, House #, address, tax payer, EMV
Other Serivces /Products	$50 to $100 per hour	GIS layers- $50 per hour; Custom created layer- $100 per hour

FAIR GROUNDS

	Fairlane Building Occupancy Max: 230 w/ tables/chairs	Floral Hall	4-H Building	Livestock Building	Comm. Building	Grounds / Shows / Rally's / Etc.
		Not Available after October 1st				
Garage Sale/Estate Sale - 3 Day Rental	$350	$350	$350	$350	$350	
Addl set up day	$50/day					
Garbage Fee	$50					
$125/day for less than 3 days						
Security Deposit	$150	$150	$150	$150	$150	
Flea Market/Auction	$450	$450	$450	$450	$450	
3 day rental						
Addl set up days	$75/day					
Garbage Fee	$50					
Security Deposit	$150	$150	$150	$150	$150	Case x Case Basis
Grad/Shower/B-Day/Baptism	$45/hour					
Minimum Charge - $225 (5 hours)		Not Available	Not Available	Not Available	Not Available	
Max - $450/day						
Security Deposit	$150					
Wedding Reception	$1,200	$1,000	$1,000	$1,000	$1,000	
Rental - Friday/Saturday/Sunday (until 10:00 a.m. only)						
Addl set up days (for full rental)	$75/day	$75/day	$75/day	$75/day	$75/day	
1 Day only rental (no addl days)	$800					
Security Deposit	$350	$350	$350	$350	$350	
Garbage/Electric Included						
Building Comments						
Tables /Chairs Available	Yes	Some tables, no chairs	Minimal Tables/Chairs	None	None	
Bathrooms	Yes	No	Yes	Yes	No	
Sink	Yes	Small Sink	No	No	No	
Refrigerator	Yes	No	No	No	No	
A/C / Heat	Yes	No	No	No	No	
Approximate Size of Building	60x80	54x150	75x150	60x150	50x125	
Full Kitchen	Yes	No	No	No	No	

EXHIBIT D

Freeborn County Data Protection Policy
(adopted effective July 19, 2022)

Part 1. Policy. The adoption of this policy by Freeborn County, Minnesota (hereafter, the "County") satisfies the requirement in Minnesota Statutes, §13.05, Subd. 5, to establish procedures ensuring appropriate access to not public data. By incorporating employee access to not public data in the County's Data Inventories (required by Minnesota Statutes, §13.025, Subd. 1), in the individual employee's position description, or both, the County's policy limits access to not public data to employees whose work assignment reasonably requires access. This policy applies to all County Departments and Offices regardless of the Responsible Authority.

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

Erin O'Brien
Assistant Freeborn County Attorney
Erin.Obrien@co.freeborn.mn.us
Phone: 507-377-5192
Fax: 507-377-5196
411 South Broadway
P.O. Box 1147
Albert Lea, MN 56007

Part 2. Procedures

Subpart A. Data inventory.

The County has prepared Data Inventories which identify and describe all not public data on individuals maintained by the County pursuant to Minnesota Statutes, §13.025, Subd. 1.

The County Administrator has established safeguards for Data Inventories to ensure the employees who have access to not public data are in compliance with §13.05, Subd. 5 have work assignments which reasonably require access.

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 County's Data Inventories, the Responsible Authority, the DPCO, the Department Heads, the Freeborn County Attorney's Office

members, and outside legal counsel retained by the County may have access to *all* not public data maintained by the County when their work assignment reasonably requires access to the data.

Subpart B. Employee position descriptions.

Position descriptions may authorize employee access to not public data when a work assignment reasonably requires it.

Subpart C. 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, §13.04) or the County 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.

Subpart D. Ensuring that not public data are not accessed without a work assignment.

Within the County, departments/offices may assign tasks by employee or by job classification. If a department/office maintains not public data to which any employee within the department/office lacks authorized access, the department/office will ensure that the not public data are secure from unauthorized access by any such employee. This policy also applies to unauthorized access of data by employees in other departments/offices that share a workspace where not public data are maintained.

Recommended procedures for preventing unauthorized 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/placing not public documents in confidential shred box when disposing of them

Part 3. Penalties for unlawfully accessing not public data.

The County may impose penalties for unlawful access to not public data including suspension, dismissal, other disciplinary action, or referral to the appropriate prosecutorial authority for consideration of criminal charges.

EXHIBIT E

Freeborn County Data Breach Notification Policy

(adopted effective July 19, 2022)

Part 1. Purpose. This policy is intended to assist Freeborn County, Minnesota and its departments and offices (hereafter the "County") to implement the requirements of Minnesota Statutes § 13.055 and provide timely and appropriate notice to individuals who are affected by a breach of the security of their private or confidential data. All County employees must immediately report known or suspected breaches of security to the employee's supervisor, department head, or the Responsible Authority. The Freeborn County Attorney's Office (CAO) in consultation with the Responsible Authority, County Administration, and/or other appropriate County personnel shall determine whether notice of the breach is required and how the notice will be communicated.

Part 2. Applicability. This policy applies to breaches of the security of private or confidential data maintained by or on behalf of the County.

Part 3. Guidelines.

Subpart A. Responsible Authority. The Responsible Authority is responsible for compliance with this Policy. The Reasonable Authority is responsible for compliance with this Policy. The Responsibility Authority will oversee the implementation of the Policy, including:

- appropriate notice and training for the workforce;
- appropriate notice and consultation with County personnel;
- periodic review of the procedures; and
- the creation and maintenance of documents in accordance with County records retention schedules.

The Responsible Authority may delegate implementation responsibilities to other County personnel as appropriate.

Subpart B. Reporting a Suspected Breach. Any employee or user who knows of or reasonably believes that a breach of security of private or confidential data has occurred must immediately report to their supervisor, department head or the Reasonable Authority.

Supervisors who receive a report of the breach must immediately report the incident to the department head and the Responsible Authority. The Responsible Authority must immediately notify the data owner of the reported breach, if necessary.

The report should include the date and time of the report, the date and time when the breach occurred (if known); the type of data involved; the number of affected individuals and other pertinent information.

County employees who report a breach under this policy must not be subject to retaliation. The Responsible Authority should make available to all employees information about this policy and how to report a security breach.

Subpart C. Breach Response Process. After a breach of security has been reported, the Responsible Authority must work with employee, the user, and the Department Head(s) of the employee and the user to take necessary steps to contain and control the integrity of the electronic or other data handling systems affected by the reported breach and conduct a preliminary internal assessment of the

scope of the breach. Applicable County Information Technology (IT) security procedures or other policies shall be consulted.

If the breach is suspected on a County computing system that contains or has network access to private or confidential data, the Responsible Authority shall consult with County IT personnel and consider control measures including but not limited to removing the computing system from the County Network.

1. Determining Breach. The Responsible Authority shall consult with the CAO to determine whether a breach of security of data has occurred. Due consideration should be given to the potential for damage to individuals if no breach is determined and notice is not provided.
    a) Incidents. Examples of the types of incidents that may result in a notice-triggering breach include:
        i. Evidence of unauthorized access into a system containing private/confidential data;
        ii. Missing or stolen laptop, desktop, storage device or any other information technology resource containing files with private/confidential data;
        iii. Documents containing private/confidential data sent in any form to a wrong recipient;
        iv. System containing private/confidential data that has been compromised; or
        v. Employee misuse of authorized access to disclose private or confidential data.
    b) Acquisition. Minnesota Statute § 13.055, Subd. 2 requires governmental entities to notify individuals if their private or confidential data has been or is reasonably believed to have been acquired by an unauthorized person. In making that determination, the following factors, among others, may be considered.
        i. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device or document containing unprotected private or confidential information;
        ii. Indications that the information that has been downloaded or otherwise acquired;
        iii. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported;
        iv. The encryption protection of the data, if any;
        v. Duration of exposure;
        vi. The extent to which the compromise of electronic data indicates a directed attack, such as a pattern showing the machine itself was specifically targeted; or
        vii. Indications that the attack was intended to seek and collect private or confidential data.
2. Timing of Notification. If a breach has been determined, in most instances the data owner has primary responsibility to notify affected individuals. Notice is to occur without unreasonable delay. The County should strive to provide notice within ten business days of determining that notice is required unless delay is appropriate due to:
    a) The legitimate needs of a law enforcement agency; or
    b) Measures necessary to determine the scope of the breach and restore the reasonable security of the data.

Immediate notification may be appropriate in the event of a breach that could have immediate deleterious impact on individuals whose data may have been acquired by an authorized person.

3. Contact Law Enforcement. The Responsible Authority shall consult with the CAO before contacting law enforcement agencies if the breach of security is believed to involve illegal activities. Information may be shared with law enforcement consistent with applicable data privacy laws. If law enforcement is contacted, it should be informed of the County's practice to provide notice to affected individuals within ten days. If law enforcement advises that such notice would impede an active criminal investigation, notice may be delayed. Delayed notice should be sent out as soon as law enforcement advises that it would no longer impede the criminal investigation.
4. Whom to Notify. The CAO, in consultation with appropriate County personnel, including but not limited to the user and data owner, shall determine the scope of the notice. Notice of a breach much be sent to any individual whose private or confidential data has been or is reasonably believed to have been acquired by an unauthorized person. If specific individuals cannot be identified, notice should be sent to groups of individuals likely to have been affected, such as all whose information is stored in the database or files involved in the breach. Appropriate measures should also be taken to prevent notice lists from being over-inclusive.

Subpart D. Notice.

1. Content. The Responsible Authority shall consult with the CAO on the wording of a notice. Notices shall generally be sent separate from other documents. The format should utilize subheadings and clear language.

   Notice shall include the following information:

   a) A general description of the data breach including when it occurred, to the extent known
   b) The nature of the individual's private or confidential information that was involved (not listing the specific private/confidential data).
   c) Information about what the County has done to protect the individual's private/confidential information from further disclosure.
   d) County assistance (such as website information or phone number of a County resource) for further information about the incident.
   e) Information, such as websites, about what individuals can do to protect themselves against identity theft including: contact information for nationwide credit reporting agencies; the Federal Trade Commission and appropriate state agency resources.
2. Method of Notification. The CAO, in consultation with the Responsible Authority, shall determine the appropriate method of notice as follows:
   a) Written notice by first class mail to each affected individual; or
   b) Electronic notice to each affected individual if communication normally occurs in that medium, and the procedure is otherwise consistent with the provisions regarding electronic records and signatures contained in 15 U.S.C. Sect. 7001; or
   c) Substitute notice may be provided if the cost of providing the written notice required to each affected individual would exceed $250,000, or the affected class of individuals to be notified exceeds $500,000, or the County does not

have sufficient contact information to notify affected individuals. Substitute notice consists of all of the following:

d) E-mail notice if the County has an e-mail address for the affected individuals;
e) Conspicuous posting of the notice on the County's website for a minimum of 45 days; and
f) Notifications to major media outlets that reach the general public.

Subpart E. Coordination with Credit Reporting Agencies. Credit reporting agencies (agencies) assist individuals in responding to a notice of a security breach. Such agencies should be notified in advance of sending notice of security breach incidents that may significantly increase calls to agencies for assistance.

If notice is required to be given to 1,000 or more individuals at one time, the County shall notify, without reasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis as defined in 15 U.S.C. Sect. 1681a, of the timing, distribution, and content of the notice to be sent. Such contacts shall include but not be limited to the following:

Equifax:
U.S. Consumer Services
Equifax Information Services, LLC.
Phone: 1-800-525-6285

Experian:
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
Phone: 1-888-397-3742

TransUnion:
Phone: 1-800-680-7289

Subpart F. Documentation. The Responsible Authority must complete a written summary for each reported breach, regardless of whether notice was given. The summary should be completed beginning at the time of the initial report or as soon thereafter as practical.

Where appropriate, all documentation related to the breach and investigation shall be labeled and maintained as not public pursuant to the applicable data privacy classification including, but not limited to, "security information" as defined by Minnesota Statutes §13.37, Subd. 1(a). The summary shall be retained by the Responsible Authority in accordance with the applicable records retention policy and may also be requested by the County Administration office.

Part 4. Definitions.

Subpart A. Breach of the security of the data. Breach of the security data means the unauthorized acquisition of data maintained by the County, in any medium, that compromises the security and classification of the data, but not including the good faith acquisition by an employee, contractor or agent of the system if not provided to an unauthorized person.

Subpart B. Confidential data. Confidential data means data on individuals which is made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data.

Subpart C. Contact information. Contact information means either: name and mailing address or name and e-mail address for each individual who is subject of data maintained by the County.

Subpart D. County. "County" means all department and offices of Freeborn County regardless of department head, supervisor or responsible authority as designated by the Board of Commissioners.

Subpart E. Data owner. The County individual, department or office with primary responsibility for the content or function of private or confidential data.

Subpart F. Government data. Government data means all data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use.

Subpart G. Information Technology Resources. Facilities, technologies, and information resources used for system member information proceeding, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials. This definition is not all inclusive, but rather, reflects examples of system equipment, supplies and services.

Subpart H. Individual. Individual means a natural person. In the case of a minor or an incapacitated person as defined in Minn. Stat. Sec. 524.5-102, subdivision 6, "individual" includes a parent or guardian or an individual acting as a parent or guardian in the absence of a parent or guardian.

Subpart I. Person. Person means any individual, partnership, corporation, association, business trust or a legal representative of an organization.

Subpart J. Private data. Private data means data on individuals made by statute or federal law applicable to the data (1) not public and (2) accessible to the individual subject of that data.

Subpart K. Responsible Authority. Responsible Authority is as defined in Minn. Stat. Sec. 13.01, Subd. 16.

Subpart L. Unauthorized acquisition. Also known as **"unauthorized access"**. Unauthorized acquisition means that a person has obtained government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for non-governmental purposes.

Subpart M. Unauthorized person. Unauthorized person means any person who accesses government data without permission or without a work assignment that reasonably requires the person to have access to the data.

Subpart N. User. Any individual, including but not limited to, employees, elected officials, appointees, interns, externs, administrators, independent contractors, and other unauthorized individuals using County information resources, whether or not the user is affiliated with the County.

13.025 GOVERNMENT ENTITY OBLIGATION.

Subdivision 1. **Data Inventory.** The responsible authority shall prepare an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's government entity. Forms used to collect private and confidential data may be included in the inventory. The responsible authority shall update the inventory annually to make the changes necessary to maintain the accuracy of the inventory. The inventory must be available from the responsible authority to the public according to the provisions of sections 13.03 and 15.17. The commissioner may require responsible authorities to submit copies of the inventory and may request additional information relevant to data collection practices, policies, and procedures.

Subd. 2. **Public data access policy**. The responsible authority shall prepare a written data access policy and update it no later than August 1 of each year, and at any other time as necessary to reflect changes in personnel, procedures, or other circumstances that impact the public's ability to access data.

Subd. 3. **Data subject rights and access policy.** The responsible authority shall prepare a written policy of the rights of data subjects under section 13.04 and the specific procedures used by the government entity for access by the data subject to public or private data on individuals. The written policy must be updated no later than August 1 of each year, and at any other time as necessary to reflect changes in personnel procedures, or other circumstances that impact the public's ability to access data.

Subd. 4. **Availability.** The responsible authority shall make copies of the policies required under subdivisions 2 and 3 easily available to the public by distributing free copies to the public or by posting the policies in a conspicuous place within the government entity that is easily accessible to the public or by posting on the government entity's website.

History: *2012 c 290 s 10*

Official Publication of the State of Minnesota
Revisor of Statutes