

## 804 Information Security

### I. Purpose

The purpose of this policy is to maintain an information security practice for the District.

### II. General Statement of Policy

The District has a cybersecurity program which maintains appropriate levels of access to District information through technological systems and practices. Data security practices apply to all District employees and for all District operations and activities. Unauthorized access, use, transfer, distribution, compromise or change of District data by any employee, student, or any other individual, may result in disciplinary action, which may include a recommendation for termination and other legal action.

### III. Requirement

In order to effectively implement this policy, the Superintendent, or designee, will:

1. Implement standards and procedures to effectively manage and provide necessary access to District data, while at the same time ensuring the confidentiality, integrity, and availability of the information. This policy relates to the use of and access to Fridley Public Schools' computing, network resources and data. All relevant elements in the District's Acceptable Use Policy and other related policies apply.
2. Maintain an information security program based on risk assessment that follows relevant best practices in the field of information security. This includes having developed a Fridley Incident Response Plan (FIRP) in the case it may be needed. Included in the FIRP will be procedures for the appropriate notification of individuals should the District experience a data incident.
3. Provide a structured and consistent process for employees, students and guardians to obtain necessary data access for conducting Fridley Public Schools operations.
4. Provide processes for evaluating and vetting software that interfaces with District data, including processes for evaluating third parties and their security practices.
5. The Director of Technology will assume the role of District Data Security Officer having responsibilities and authority to enforce the Information Security Policy and procedures.

## IV. Scope

1. These security processes and procedures apply to information found in or converted to a digital format.
2. Security processes and procedures apply to all employees, contract workers, volunteers, and visitors to the Fridley Public Schools and all data used to conduct operations of the District.
3. Security processes and procedures apply to District data accessed from any location; internal, external, or remote.
4. Security processes and procedures apply to the transfer of any District data inside or outside the District for any purpose.

## V. Guiding Principles

1. The Superintendent, or designee, shall determine appropriate access permissions.
2. Data users are granted data access privileges commensurate with their role and work responsibilities and are responsible for their actions while using these privileges. That is, all schools or other facilities are responsible for the District data they access, create, modify, and/or delete.
3. Any individual granted access to District data is responsible for the ethical use of that data. Access will be granted only in accordance with the authority delegated to the individual to conduct Fridley Public Schools functions.
4. It is the express responsibility of authorized users to safeguard the data they are entrusted with, their credentials, and comply with all aspects of this policy and additional related District policies and/or procedures.
5. These security measures apply to District data regardless of location. Users who transfer or transport District data “off-campus” for any reason must ensure that they are able to comply with appropriate data security measures prior to transporting or transferring the data.

### **Cross References:**

Policy #515 – Protection and Privacy of Student Records

Policy #524 – Internet Acceptable Use Policy

Policy #806 – Crisis Management Policy

### **Legal References:**

20 U.S.C. Sec. 1232g et. Seq. (Family Educational Rights and Privacy Act) Minn. Stat.

Ch. 13 (Minnesota Government Data Practices Act)

### ***Approved:***

Adopted as Policy 804 Information Security on April 19, 2022