SCHOOL POLICIES
HOPKINS SCHOOL DISTRICT 270
1001 HIGHWAY 7
HOPKINS, MINNESOTA 55305

HOPKINS PUBLIC SCHOOLS
Excellence. Every School. Every Student. Every Day.

DISTRICT CODE: 859

ELECTRONIC DATA SECURITY MEASURES

Policy reflects Minnesota statute and aligns with other District 270 policies.

I. PURPOSE

The purpose of this policy is to authorize and direct the Superintendent to establish, implement, and maintain data security measures.

II. GENERAL STATEMENT OF POLICY

The District establishes data security classifications, implements procedural and electronic security controls, and maintains records regarding assigned security authorization. Data security measures apply to District employees and all District operations. Any unauthorized access, use, transfer, or distribution of District data by any employee, student, or any other individual, may result in appropriate 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:

A. 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. Insofar as this policy deals with access to Hopkins Public Schools' computing and network resources, all relevant provisions in the District's Acceptable Electronic Use Policy apply.

B. Implement procedures to effectively and appropriately handle data breaches, including procedures to notify students and families, and notification to affected educational institutions in the case of an online service provider breach.

C. Provide a structured and consistent process for employees to obtain necessary data access for conducting Hopkins Public Schools operations.

D. Define data classification and related safeguards.

E. Provide a list of relevant considerations for system personnel responsible for purchasing or subscribing to software that will utilize and/or expose District data.

F. Establish a District Data Security Officer role appointed by the Superintendent with responsibilities and authority to enforce Hopkins Data Security Policy and procedures.

IV. SCOPE

A. These security measures apply to information found in or converted to a digital format. (The same information may exist in paper format for which the same local policies, state laws, statutes, and federal laws would apply, but no electronic control measures are needed.)

B. Security measures apply to all employees, contract workers, volunteers, and visitors of the Hopkins Public Schools and all data used to conduct operations of the District.

C. Security measures do not address public access to data.

D. Security measures apply to District data accessed from any location; internal, external, or remote.

E. Security Measures apply to the transfer of any District data inside or outside the District for any purpose.

V. GUIDING PRINCIPLES

A. The Superintendent, or designee, shall determine appropriate access permissions.

B. Data Users granted “create” and/or “update” privileges are responsible for their actions while using these privileges. That is, all schools or other facilities are responsible for the District data they create, update, and/or delete.

C. Any individual granted access to District data is responsible for the ethical use of that data. Access will be used only in accordance with the authority delegated to the individual to conduct Hopkins Public Schools operations.

D. It is the express responsibility of authorized users to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and additional related District policies and/or procedures.

E. 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 all data security measures prior to transporting or transferring the data.

VI. ACCESS COORDINATION

A. Users appointed by the Superintendent, or designee, as Data Stewards, will be responsible for assisting in classifying data sensitivity levels for their areas of expertise and in identifying which employees require access to which information in order to complete their duties.

B. The Director of Technology, Media and Information Systems will designate individuals within the technology department to implement, monitor, and safeguard access to District data based on the restrictions and permissions determined by the Data.

C. Data Stewards will be responsible for educating all employees in their areas of responsibilities associated with electronic Data security.

VII. POLICY REVIEW

The Board will annually review this policy.

Adopted: December 17, 2015

Reviewed: September 22, 2016, September 25, 2018

Revised: September 19, 2017