SUPPORT OPERATIONS 5306

PROTECTION OF STUDENT, TEACHER, AND PRINCIPAL PERSONAL INFORMATION (DATA SECURITY AND PRIVACY)

I. Statement of Policy

In order to conduct a successful education program, the District receives, creates, stores, and transfers information about students, teachers, and principals that is protected by state and federal law. The District takes active steps to protect the confidentiality of protected information in compliance with all applicable state and federal laws. The District expects all District officers, employees, and partners to maintain the confidentiality of protected information in accordance with state and federal law and all applicable Board Policies.

This Policy shall be published on the District website.

II. Scope of Policy

A. Protected Information

1. The term Protected Information used in this Policy includes both, Protected Student Information, and Protected Teacher and Principal Information that is recorded in any form, including paper or digital, and text or image or sound.

2. The term Protected Student Information means personally identifiable information as defined in the federal regulations implementing the Family Educational Rights and Privacy Act (FERPA), found at 34 C.F.R. Section 99.3.

3. The term Protected Teacher and Principal Information means personally identifiable information about an individual's Annual Professional Performance Review (APPR) rating, as described in Education Law Section 3012-c(10).

B. Affected Persons and Entities

1. The term Student includes any person attending school in an educational agency, or seeking to become enrolled in an educational agency.

2. The term Parent includes the parent, legal guardian, or person in parental relation to a Student.

3. The term Data Subject includes any Student and the Parent of the Student, and any teacher or principal who is identified in Protected Information held by the District.

4. As used in this Policy, the term Third Party means any person or organization that (a) is not employed by this District and is not an Educational Agency and (b) receives Protected Information from this District. The term Third Party includes for-profit organizations, not-for-profit organizations, higher education institutions, and governmental agencies that are not Educational Agencies (such as law enforcement agencies).

5. As used in this Policy, the term Educational Agency includes public school districts, boards of cooperative educational services, charter schools, the State Education Department, certain pre-k programs, and special schools described in Section 2-d of the Education Law; higher education institutions are not Educational Agencies for purposes of this Policy.

C. Other Important Definitions

1. The term Breach means the unauthorized acquisition of, access to, use of, or disclosure of Protected Information by or to a person who is not authorized to acquire, access, use, or receive that Protected Information.

2. A Disclosure of Protected Information occurs when that information is released, transferred, or otherwise communicated to an unauthorized party by any means, including oral, written, or electronic; a disclosure occurs whether the exposure of the information was intentional or unintentional. A Disclosure is Unauthorized if it is not permitted by state or federal law or regulation, or by any lawful contract, or not made in response to a lawful order of a court or tribunal.

3. The term Commercial or Marketing Purpose means (a) the sale of Protected Student Information, (b) the use or disclosure of Protected Student Information by any party (including the District) for purposes of receiving remuneration, either directly or indirectly, (c) the use of Protected Student Information for advertising purposes, (d) the use of Protected Student Information to develop or improve a Third Party product or service, or (e) the use of Protected Student Information to market products or services to students.

D. Implementation with Other Policies and Laws

The District has adopted other Policies and practices to comply with state and federal laws such as FERPA, IDEA, and the National School Lunch Act. This Policy will be implemented to supplement, and not replace, the protections provided by those laws, as recognized in District Policies and practices.

III. General Principles for Use and Security of Protected Information

A. Intentional Use of Protected Information

1. All District staff and officers are expected to receive, create, store, and transfer the minimum amount of Protected Information necessary for the District to implement its education program and to conduct operations efficiently. In particular, the number of email documents containing Protected Information should be minimized.

2. Protected Student Information will only be disclosed to other District staff or Third Parties when that person or entity can properly be classified as a school official with a legitimate educational interest in that Protected Information, meaning that the person or entity requires that information to perform their job or fulfill obligations under a contract with the District.

3. Protected Information shall not be disclosed in public reports or other public documents.

4. Before Protected Student Information is disclosed to a Third Party, there shall be a determination that the disclosure of the Protected Information to that Third Party will benefit the student(s) whose information is being disclosed and the District.

5. Except as required by law or in the case of educational enrollment data, the District shall not report to the State Education Department student juvenile delinquency records, student criminal records, student medical and health records, or student biometric information.

B. Commercial and Marketing Use of Protected Information Prohibited

The District shall not sell protected information or use or disclose protected information for the purpose of receiving remuneration either directly or indirectly. The District shall not facilitate the use of Protected Information by another party for that party's commercial or marketing purpose.

IV. Data Protection Officer

A. Board Designation

Upon the recommendation of the Superintendent, the Board will designate a Data Protection Officer. The designation shall be made by formal action at a Board meeting.

B. Responsibilities of Data Protection Officer

1. The Data Protection Officer shall be responsible for the implementation of this Policy, under the supervision of the Superintendent, if not the Superintendent, and consistent with other Board Policies.

2. The Data Protection Officer shall serve as the initial point of contact for data security and privacy matters affecting the District, including communications with the Chief Privacy Officer of the State Education Department.

3. In addition to specific responsibilities identified in this Policy, the Data Protection Officer shall oversee the District assessment of its risk profile and assist the Superintendent, if not the Superintendent, in identifying appropriate steps to decrease the risk of Breach or Unauthorized Disclosure of Protected Information, in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

V. Actions to Reduce Cybersecurity Risk

A. NIST Cybersecurity Framework

1. The District shall plan, install, maintain, operate, and upgrade its digital information network systems, infrastructure, and practices in alignment with the NIST Cybersecurity Framework, version 1.0, with the goal of steadily reducing the risk of unauthorized disclosure of, or access to, the Protected Information stored on and transmitted through the network.

2. In accordance with the approach of the NIST Cybersecurity Framework, the Superintendent shall direct appropriate District personnel, including the Data Protection Officer, to continually assess the current cybersecurity risk level of the District, identify and prioritize appropriate “next steps” for the District to take to reduce cybersecurity risk, and implement actions

to reduce that risk, consistent with available fiscal and personnel resources of the District.

3. Decisions regarding procurement and implementation of hardware and software, and decisions regarding the collection and use of Protected Information, shall take into consideration the anticipated benefit to the education program or operations of the District, and the potential increase or decrease in the risk that Protected Information will be exposed to unauthorized disclosure.

B. Setting Expectations for Officers and Employees

1. Notice of this Policy shall be given to all officers and employees of the District.

2. Officers and employees of the District shall receive cybersecurity training designed to help them identify and reduce the risk of unauthorized disclosures of Protected Information. Each employee shall receive such training at least annually. This training shall include information about the state and federal laws that govern Protected Information and how to comply with those laws and meet District expectations for use and management of Protected Information.

VI. Parents Bill of Rights for Data Privacy and Security

A. Content of the Parents Bill of Rights for Data Privacy and Security

The District publishes on its website and will maintain a Parents Bill of Rights for Data Privacy and Security that includes all elements required by the Commissioner's Regulations, including supplemental information about data-sharing agreements as described in Part B below.

B. Public Access to the Parents Bill of Rights for Data Privacy and Security.

The Parents Bill of Rights for Data Privacy and Security shall be posted on the District website. The website copy of the Parents Bill of Rights for Data Privacy and Security shall include links to the following supplemental information about each contract between the District and a Third Party that receives Protected Information:

1. The exclusive purpose(s) for which the District is sharing the Protected Information with the Third Party;

2. How the Third Party will ensure that any other entities with which it shares the Protected Information, if any, will comply with the data protection and security provisions of law and the contract;

3. When the agreement expires and what happens to the Protected Information when the agreement expires;

4. That a Data Subject may challenge the accuracy of the Protected Information through the process for amending education records under the Education Records Policy of the District (Protected Student Information) or the appeal process under the APPR Plan of the District (Protected Teacher and Principal Information);

5. Where the Protected Information will be stored (described in a way that protects data security); and

6. The security protections that will be taken by the Third Party to ensure that the Protected Information will be protected, including whether the data will be encrypted.

VII. Standards for Sharing Protected Information with Third Parties

A. Written Agreement For Sharing Protected Information With a Third Party Required

1. Protected Information shall not be shared with a Third Party without a written agreement that complies with this Policy and Section 2-d of the Education Law.

2. Disclosing Protected Information to other educational agencies does not require a specific written agreement, because educational agencies are not Third Parties. However, any such sharing must comply with FERPA and Board Policy.

3. When the District uses a cooperative educational services agreement (CoSer) with a BOCES (the CoSer BOCES) to access an educational technology platform that will result in Protected Information from this District being received by a Third Party, this District will confirm that the product is covered by a contract between the CoSer BOCES and the Third Party that complies with Education Law Section 2-d. This District will confirm with the CoSer BOCES the respective responsibilities of this District and the CoSer BOCES for providing breach notifications and publishing supplemental information about the contract.

B. Review and Approval of Online Products and Services Required

1. District staff do not have authority to bind the District to the Terms of Use connected to the use of online software products, regardless of whether there is a price attached to the use of the online product. Any staff member considering the use of an online product to perform the duties of their position should carefully read the online Terms of Service to determine whether accepting those terms will be considered binding on the District by the vendor.

2. If the use of an online product will result in the vendor receiving Protected Information, then the vendor is a Third Party and any agreement to use the online product must meet the requirements of this Policy and Education Law Section 2-d. **Therefore, no staff member may use an online product that shares Protected Information until use of that product has been reviewed and approved by the Data Protection Officer.**

3. The Superintendent and/or the Data Protection Officer, shall establish a process for the review and approval of online technology products proposed for use by instructional or non-instructional staff.

C. Minimum Required Content for Third Party Contracts

1. Protected Information may not be shared with a Third Party unless there is a written, properly authorized contract or other data-sharing agreement that obligates the Third Party to:

a. maintain the confidentiality of the Protected Information in accordance with all applicable state and federal laws;

b. maintain the confidentiality of the Protected Information in accordance with this Policy;

c. use the shared Protected Information only for the purpose(s) specifically described in the contract, and to not use the Protected Information for any Commercial or Marketing Purpose;

d. limit access to Protected Information to only those officers and employees who need access in order to perform their duties in fulfilling the contract on behalf of the Third Party;

e. ensure that no officer or employee of the Third Party will be given access to Protected Information until they have received training in the confidentiality requirements of state and federal laws and this Policy;

f. not disclose any Protected Information to any other party who is not an authorized representative of the Third Party using the information to carry out Third Party's obligations under the contract, unless (i) Third Party has the prior written consent of the Data Subject to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

g. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

h. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

i. notify the District of any breach of security resulting in an unauthorized release of Protected Information by the Third Party or its assignees in violation of state or federal law, or in violation of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

j. where a breach or unauthorized disclosure of Protected Information is attributed to the Third Party, the Third Party shall pay for or promptly reimburse the District for the full cost incurred by this District to send notifications required by the Education Law.

2. The contract or other data-sharing agreement with the Third Party must include the Third Party's Data Security and Privacy Plan that is accepted by the District. The Plan must include a signed copy of the District Parents Bill of Rights for Data Privacy and Security, and shall:

a. warrant that the Third Party's practices for cybersecurity align with the NIST Cybersecurity Framework 1.0;

b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

c. outline how the Third Party will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with this Policy;

d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under the contract;

e. demonstrate that it complies with the requirements of Section 121.3(c) of the Commissioner's Regulations;

f. specify how officers or employees of the Third Party and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

g. specify if the Third Party will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

h. specify how the Third Party will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District; and

i. describe whether, how, and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Third Party when the contract is terminated or expires.

3. The contract or other data-sharing agreement with the Third Party must also include information sufficient for the District to publish the supplemental information about the agreement described in Part VI-B of this Policy.

VIII. District Response to Reported Breaches and Unauthorized Disclosures

A. Local Reports of Possible Breach or Unauthorized Disclosures

1. Data Subjects and other District staff who have information indicating that there has been a Breach or Unauthorized Disclosure of Protected Information must report that information to the Data Protection Officer.

2. The report of suspected Breach or Unauthorized Disclosure must be made in writing. A report received by email will be considered a written report. The report shall provide as much information as is available to the reporting party concerning what Protected Information may have been compromised, when and how the possible Breach or Unauthorized Disclosure was discovered, and how the Data Privacy Officer may contact the reporting party. The Data Protection Officer shall make a form available online and in each school office to be used for reporting a suspected Breach or Unauthorized Disclosure.

3. The Data Protection Officer, or designee, shall take the following steps after receiving a report of a possible Breach or Unauthorized Disclosure of Protected Information:

a. promptly acknowledge receipt of the report;

b. determine, in consultation with appropriate technical staff, what, if any, technology-based steps should be taken immediately to secure against further compromise of Protected Information;

c. conduct a thorough factfinding to determine whether there has been a Breach or Unauthorized Disclosure of Protected Information, and, if so, the scope of the Breach or Unauthorized Disclosure and how it occurred;

d. if a Breach or Unauthorized Disclosure of Protected Information is found to have occurred, implement the Cybersecurity Incident Response Plan to correct and ameliorate the Breach or Unauthorized Disclosure and provide appropriate notifications to the SED Chief Privacy Officer and affected Data Subjects; and

e. when the factfinding process is complete, provide the reporting party with the findings made at the conclusion of the factfinding process; this should occur no later than 60 days after the receipt of the initial report, and, if additional time is needed, the reporting

party shall be given a written explanation within the 60 days that includes the approximate date when the findings will be available.

4. The Data Protection Officer shall maintain a record of each report received of a possible Breach or Unauthorized Disclosure, the steps taken to investigate the report, and the findings resulting from the investigation in accordance with applicable record retention policies, including Records Retention and Disposition Schedule ED-1.

5. When this reporting and factfinding process results in confirmation of a Breach or Unauthorized Disclosure of Protected Information, the Data Protection Officer, or designee, shall follow the notification procedures described in Part VIII. B., below.

6. The availability of this process for reporting suspected Breaches or Unauthorized Disclosures of Protected Information shall be communicated to all staff and all student households, in addition to the general posting of this Policy on the District website.

B. Notification of Breach or Unauthorized Disclosure of Protected Information

1. Third Parties who learn of the Breach or Unauthorized Disclosure of Protected Information received from the District are required by law to notify the District of that occurrence no more than seven days after their discovery of the Breach or Unauthorized Disclosure. When the District receives such a notification, the Data Protection Officer, or designee, shall promptly obtain from the Third Party the following information if it is not already included in the notice:

   a. a brief description of the Breach or Unauthorized Disclosure;

   b. the dates of the incident;

   c. the dates of the discovery by the Third Party;

   d. the types of Protected Information affected; and

   e. an estimate of the number of records affected.

2. When the District is notified by a Third Party of a Breach or Unauthorized Disclosure of Protected Information in the custody of the Third Party, the Data Protection Officer shall notify the Chief Privacy Officer of the State Education Department of that information within ten calendar days of

receiving it from the Third Party, using the form provided by the Chief Privacy Officer.

3. When the District learns of an Unauthorized Disclosure of Protected Information originating within the District, whether as the result of a report made under this Policy or otherwise, the Data Protection Officer shall notify the Chief Privacy Officer of the State Education Department of that information within ten calendar days of discovering the Unauthorized Disclosure, using the form provided by the Chief Privacy Officer.

4. When the District has received notification from a Third Party of a Breach or Unauthorized Disclosure of Protected Information, or has otherwise confirmed that a Breach or Unauthorized Disclosure of Protected Information has occurred, the District shall notify all affected Data Subjects by first class mail to their last known address, by email, or by telephone, of the Breach or Unauthorized Disclosure. Notifications by email shall be copied into the record of the incident. Logs of telephone notifications shall be maintained with each record signed by the District employee making the contact. Each notification shall include the following information:

   a. each element of information described in paragraph 1 above,

   b. a brief description of the District investigation of the incident or plan to investigate; and

   c. contact information for the Data Protection Officer as a point of contact for any questions the Data Subject may have.

5. The notification of affected Data Subjects shall be made in the most expedient way possible and without unreasonable delay, but no later than 60 calendar days after the discovery of the Breach or Unauthorized Disclosure or the receipt of the notice from the Third Party. If notification within the 60 day period would interfere with an ongoing law enforcement investigation or would risk further disclosure of Protected Information by disclosing an unfixed security vulnerability, notification may be delayed until no later than seven calendar days after the risk of interfering with the investigation ends or the security vulnerability is fixed.

6. Where notification of affected Data Subjects is required because of a Breach or Unauthorized Disclosure attributed to a Third Party, the Data

Protection Officer shall prepare and submit to the Third Party a claim for reimbursement, as provided in Section 2-d of the Education Law.

7. Where notification of affected Data Subjects is required because of a Breach or Unauthorized Disclosure of Protected Information under this Policy, the Data Protection Officer shall also determine whether the District is required to provide any notifications pursuant to the Information Security Breach policy.

==========

New York Mills Union Free School District

Legal Ref: NYS Education Law Section 2-d; Family Educational Rights and Privacy Act FERPA 20 U.S.C. 1232g

Cross Ref: 7500, Education Records
5303, Information Security Breach

Adopted: 07/07/20