SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The District is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The District adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align the District's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

1. The term Protected Information as used in this Policy means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d.

2. The term Student as used in this Policy means any person attending school in an educational agency or seeking to become enrolled in an educational agency.

3. The term Eligible Student means a student eighteen years or older.

4. The term Parent includes either natural or adoptive parent of a student unless his or her rights under the FERPA (Family Educational Rights and Privacy Act) have been removed by court order; state statute or legally binding document relating to such matters as divorce, separation or custody that specifically revokes these rights, a guardian, or an individual acting as a parent or guardian in the absence of the student's parent or guardian.

5. As used in this Policy, Third-Party Contractor means any person or entity, other than an Educational Agency, that receives student data or teacher or Principal data from the Otego-Unadilla School District pursuant to a contract or other written agreement for purposes of providing services to the Educational Agency, including, but not limited to, data management or storage services, conducting studies for or on behalf of the Educational Agency, or audit or evaluation of publicly funded programs.

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

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

7. 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.

8. A Disclosure of Protected Information occurs when that information is released, transferred or otherwise communicated to an authorized 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.

9. As used in this Policy, the term Commercial or Marketing Purpose means:
    a. the sale of Protected Information,
    b. the use or disclosure of Protected Information by any party (including the Otego-Unadilla School District) for purposes of receiving remuneration, either directly or indirectly,
    c. the use of Protected Information for advertising purposes,
    d. the use of Protected Information to develop or improve a Third-Party product or service,
    e. the use of Protected Information to market products or services to students.

Implementation with Other Policies and Laws

The Otego-Unadilla School District has adopted other Policies and practices to comply with State and federal laws. This Policy will be implemented to supplement, and not replace, the protections provided by those laws, as recognized in Otego-Unadilla School District Policies and practices.

Nothing contained in this Policy or the Otego-Unadilla School District Parents' Bill of Rights for Data Security and Privacy shall be construed as creating a private right of action against the Otego-Unadilla School District.

General Principles for Use and Security of Protected Information

1. Intentional Use of Protected Information
    a. The Otego-Unadilla School District shall take steps to minimize its collection, process and transmission of Protected Information. All Otego-Unadilla School District staff and officers are expected to receive, create, store and transfer the minimum amount of protected Information necessary for Otego-Unadilla School District to implement its education program and to conduct operations efficiently.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

b. Protected Information will only be disclosed to other Otego-Unadilla School 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 information to perform their job or fulfill obligations under a contract with the Otego-Unadilla School District.

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

d. Except as required by law or in the case of enrollment data, the Otego-Unadilla School District shall not report to NYSED Juvenile Delinquency records, criminal records, medical health records, or student biometric information.

e. Every use and disclosure of personally identifiable information, as defined by FERPA, shall be for the benefit of students and the educational agency.

2. Commercial and Marketing Use of Protected Information is Prohibited:
The Otego-Unadilla School District shall not sell or disclose for marketing or commercial purposes any Protected Information or facilitate its use of disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

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

Actions to Reduce Cybersecurity Risk
1. NIST Cybersecurity Framework
   a. The Otego-Unadilla School District hereby adopts the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) in accordance with the Commissioner's Regulations.

   b. In accordance with the approach of the NIST Cybersecurity Framework, the District Superintendent shall direct appropriate Otego-Unadilla School District personnel to continually assess the current cybersecurity risk level of the Otego-Unadilla School District, identify and prioritize appropriate "next steps" for the Otego-Unadilla School District to take to reduce cybersecurity risk, and implement actions to reduce that risk, consistent with available fiscal and personnel resources of the Otego-Unadilla School District.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

2. Setting Expectations for Officers and Employees
    a. This Policy shall be published on the Otego-Unadilla School District's website and notice of the policy will be provided to all officers and employees of the district.

    b. Officers and employees of the Otego-Unadilla School District shall receive annual privacy and security awareness training inclusive of State and federal laws that govern Protected Information and how to comply with those laws and meet Otego-Unadilla School District expectations for use and management of Protected Information.

Parents' Bill of Rights for Data Privacy and Security

1. Contents of the Parents' Bill of Rights for Data Privacy and Security:
   The Otego-Unadilla School 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.

2. Public Access to the Parents' Bill of Rights for Data Privacy and Security
    a. Every contract or written agreement with a Third-Party Contractor under which the Third-Party Contractor will receive Protected Information shall include a signed copy of the Otego-Unadilla School District Parents' Bill of Rights for Data Privacy and Security and supplemental information that is sufficient for the Otego-Unadilla School District to publish on its website.

    b. The Otego-Unadilla School District shall provide the data protection as well as the protection of parent and eligible student's rights and rights to challenge the accuracy of such data required by FERPA (20 USC §1232g, IDEA (20 USC §1400 et. Seq.) and any implementing regulations. Procedures for reviewing student records can be found in the Board Policy 6420 entitled Student Records: Access and Challenge. Students and parents should be aware that requests may be referred to the home district.

Standards for Sharing Protected Information with Third-Party Contractors

1. Written Agreement for Sharing Protected Information With a Third-Party Required
    a. Protected Information shall not be shared with a Third-Party unless there is a written, properly authorized contract or other agreement that complies with this Policy and Section 2-d of New York State Education Law.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

b. Every contract or written agreement with a Third-Party Contractor under which the Third-Party contractor will receive Protected Information shall include a data security and privacy plan that outlines how all State, federal and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with this Policy.

c. All contracts or written agreements with Third-Party Contractors that have access to Protected Information shall comply with the NIST Cybersecurity Framework in accordance with the Commissioner's Regulations.

d. 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.

e. When the Otego-Unadilla School District makes an agreement with another School District to access an educational technology platform that will result in Protected Information from the Otego-Unadilla School District being received by a Third-Party, the Otego-Unadilla School District will confirm that the product is covered by a contract or written agreement between the Otego-Unadilla School District and the Third-Party that complies with Section 2-d of New York State Education Law. The Otego-Unadilla School District will confirm with the other School District the respective responsibilities of the Otego-Unadilla School District and the other School District for providing breach notifications and publishing supplemental information about the contract.

2. Review and Approval of Online Products and Services Required:
The District Superintendent, in consultation with appropriate Otego-Unadilla School District personnel, shall establish a process for the review and approval of online technology products proposed for use by instructional and non-instructional staff.

District Response to Reported Breaches and Unauthorized Disclosures

1. Local Reports of Possible Breach or Unauthorized Disclosures
   a. Student(s), Eligible Student(s), Parent(s), teacher(s) or Principals and other Otego-Unadilla School District staff who have information indicating there has been a Breach or Unauthorized Disclosure of Protected Data may report that information to the Data Protection Officer.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

b. 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 Protection 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.

c. 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:

i. promptly acknowledge receipt of the report;
ii. 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;
iii. conduct a thorough fact-finding 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;
iv. 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 NYSED Chief Privacy Officer and affected persons; and
v. when the fact-finding process is complete, provide the reporting party with the findings made at the conclusion of the fact-finding 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.

d. 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.

e. When this reporting and fact finding 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 2. Notification of Breach or Unauthorized Disclosure of Protected Information, below.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

f. The availability of this process or 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 Otego-Unadilla School District's website.

2. Notification of Breach or Unauthorized Disclosure of Protected Information
   a. Third-Parties who learn of the Breach or Unauthorized Disclosure of Protected Information received from the Otego-Unadilla School District are required by law to notify the Otego-Unadilla School District of that occurrence no more than seven days after their discovery of the Breach or Unauthorized Disclosure. When the Otego-Unadilla School 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:
      i. a brief description of the Breach or Unauthorized Disclosure;
      ii. the dates of the incident;
      iii. the dates of the discovery by the Third Party;
      iv. the types of Protected Information affected; and
      v. an estimate of the number of records affected.

   b. When the Otego-Unadilla School 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 NYSED Chief Privacy Officer of that information within ten calendar days of receiving it from the Third-Party, using the form provided by the NYSED Chief Privacy Officer.

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

   d. When the Otego-Unadilla School 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 Otego-Unadilla School District shall notify all affected individuals 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

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

incident. Logs of telephone notifications shall be maintained with each record signed by the Otego-Unadilla School District employee making the contact. Each notification shall include the following information:

i. each element of information described in paragraph a. above,
ii. a brief description of the Otego-Unadilla School District investigation of the incident or plan to investigate; and
iii. contact information for the Data Protection Officer as a point of contact for any questions the individual(s) may have.

e. The notification of affected individuals 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.

f. Where notification of affected individuals 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 New York State Education Law.

g. Where notification of affected individuals is required because of a Breach or Unauthorized Disclosure of Protected Information under this Policy, the Data Protection Officer shall also determine whether the Otego-Unadilla School District is required to provide any notifications pursuant to the Notification of Breach of Security Policy.

Also see: Policy 3120 – Web Page Policy
Policy 3320 – Privacy Policy
Policy 6410 – Staff Use of Computerized Resources
Policy 7240 – Student Records: Access and Challenge
Policy 8271 – Internet Protection Policy

First Reading: June 1, 2020
Second Reading/Adopted: June 15, 2020