Bill of Rights for Data Security and Privacy

Morris Central School District

PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

As used in this policy, the following terms are defined:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Third Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of an educational partnership organization that receives student or teacher or Principal data from a school district to carry out is responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or Principal data will be sold or released for any commercial purpose;
2. Parents have the right to inspect and review the complete contents of their child's education records. Procedures for reviewing student records can be found in the Board Policy entitled (insert title of FERPA policy);
3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d(5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cyber security Version 1.1 (NIST Cyber security Framework or NIST CSF) is adopted as the standard for data security and privacy;
4. New York state maintains a complete list of all student data collected by the State and the data is available for public review at http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234;
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaint may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure.

6. The District has also established the following procedures for parents to file complaints with the District about breaches or unauthorized releases of student data:
    a. All complaints must be submitted to the District's Data Protection Officer in writing.
    b. Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.
    c. Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;
    d. Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;
    e. The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.
7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:
    a. the exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;
    b. how he third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outline in applicable State and federal laws and regulations)e.g., FERPA; Education Law §2-d);
    c. the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District, and whether, when and how the data will be destroyed?;
    d. if and how a parent, student eligible student, teacher or Principal may challenge the accuracy of the student data or teacher or Principal data that is collected;
    e. where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.