Data Security and Privacy Policy

The Board of Education acknowledges its obligations under Education Law §2-d and the need to maintain security and privacy of student data and teacher or principal Annual Professional Performance Review Data.

The Board shall designate a Data Protection Officer ("DPO") who will be responsible for the implementation of the policies and procedures required under Education Law §2-d and its accompanying regulations. The DPO shall serve as the point of contact for data security and privacy for the District. The contact information for the DPO shall be posted on the District's website.

The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The District's DPO is responsible for ensuring the District complies with its obligations to implement data safeguards in compliance with NIST CSF and Education Law §2-d.

The Board of Education has adopted a Parent's Bill of Rights for Data Privacy and Security ("Parent's Bill of Rights"). The Parent's Bill of Rights is published on the District's website at [insert web address] and can be requested from the District Clerk.

A. Compliance with Law

The District shall comply with the New York State, federal and local laws, rules and regulations concerning the collection, retention, dissemination, destruction, disclosure, confidentiality and security of Student Data, which is defined as Personally Identifiable Information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g. Specifically, the District will comply with the applicable New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. All requests to inspect and review educational records shall be made in writing.

Every use and disclosure of Student Data will be for the benefit of the student and the District (e.g. improve academics, empower parents and students with information and/or advance efficient and effective school operations). Student Data will not be included in public reports or other documents.

The District shall comply with the New York State law concerning the disclosure, confidentiality, and security of Teacher or Principal APPR Data, which is defined as Personally Identifiable Information from the records of an Educational Agency 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. Teacher or Principal APPR Data will not be included in public reports or other documents.

B. Security Breach

The District shall respond to a Student Data or Teacher or Principal APPR Data breach by the District or a Third-Party Contractors in accordance with an Incident Response Plan maintained by the District's DPO. A "Data Breach" shall be defined as an unauthorized acquisition, access, use, or disclosure of Student Data or Teacher or Principal APPR Data in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a breach of District's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Student Data or Teacher or Principal APPR Data. All complaints concerning an actual or potential Data Breach must be submitted to the District's Data Protection Officer and the Superintendent of Schools in writing. The District's complaint procedure will be posted on the District's website. The District will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about a potential Data Breach to the Chief Privacy Officer at NYSED.

C. Third Party Contractors

The District will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive Student Data or Teacher or Principal APPR Data from the District, the contract or written agreement will include provisions requiring the confidentiality and security of shared Student Data or Teacher or Principal APPR Data in compliance with applicable law.

The District shall include provisions in contracts or written agreements with Third Party Contractors prohibiting: (1) the sale, use or disclosure of Student Data or Teacher or Principal APPR Data for any marketing or commercial purposes; (2) acts facilitating the use or disclosure of Student Data or Teacher or Principal APPR Data by any other party for any marketing or commercial purpose; and/or (3) the authorization of another party to take such actions.

D. Training

The District will provide annual training on data privacy and security awareness to its officers andl employees with access to Student Data or Teacher or Principal APPR Data. Such training will include training on state and federal laws that protect Student Data or Teacher or Principal APPR Data, and how employees can comply with such laws.

This Policy shall be posted on the District's website, with notice of the Policy provided to all officers and employees.