Data Security and Privacy Policy (to be enacted by July 1, 2020)

(Required for Districts and BOCES)

Definitions:

1. Protected Data means personally identifiable data 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.

Requirements:

1. Publication: This policy shall be published on the District's website and notice of the policy provided to all officers and employees of the District.
2. The 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.
3. The District hereby adopts the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) in accordance with the Commissioner's Regulations.
4. Every contract or other written agreement with a third party contractor under which the third party contractor will receive protected student data or teacher or Principal data 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.
5. Nothing contained in this policy or the District's Data Security and Privacy Plan shall be construed as creating a private right of action against the District.
6. Every use and disclosure of personally identifiable information, as defined by FERPA, shall be for the benefit of students and the educational agency. Examples of such benefit are provided in implementing regulations.
7. The District shall not sell or disclose for marketing or commercial purposes any Protected Data, or facilitate its use of disclosure by any other party for any marketing or commercial purpose, or permit another party to do so.
8. The District shall take steps to minimize its collection, process and transmission of Protected Data.
9. Except as required by law or in the case of enrollment data, the District shall not report to NYSED Juvenile Delinquency records, criminal records, medical health records, or student biometric information.
10. All contracts with vendors that have access to Protected Data shall comply with NIST Cybersecurity Framework.