NYS ED LAW 2-D DATA PROTECTION & PLANNING

VERSION DATE: OCTOBER 1, 2020 **|** **ELECTRONIC VERSION:** https://riconedpss.org/

RIC one

TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE

NYS REQUIREMENTS FOR DATA SECURITY AND PRIVACY

Education Law 2-d and Part 121 of the Commissioner's Regulations outline requirements for school districts and BOCES related to the protection of the personally identifiable information (PII) of students, as well as some teacher and principal information. The law and the regulations require schools to undertake a multi-pronged approach to information governance.

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Protect the confidentiality of student PII (as defined in FERPA) and certain teacher and principal PII (confidential APPR data)

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Develop and post, on the agency's website, a Parents Bill of Rights with supplemental information about each agreement with a third-party contractor that involves disclosure of PII

DATA SECURITY AND PRIVACY POLICY

Adopt and post a Data Security and Privacy Policy that includes adherence to the NIST Cybersecurity Framework to protect PII

NIST CYBERSECURITY FRAMEWORK

Apply the planning, processes, and categories of information protection defined within the NIST Cybersecurity Framework to district practices

THIRD-PARTY CONTRACTS

Whenever a contractor receives protected PII, ensure that the agreement for using the product or services (or, an addendum to that agreement) includes required language

ANNUAL EMPLOYEE TRAINING

Deliver annual privacy and security awareness training to all employees with access to protected data

UNAUTHORIZED DISCLOSURE COMPLAINT PROCEDURES

Create and publish a complaint process

INCIDENT REPORTING AND NOTIFICATION

Follow reporting and notification procedures when a breach or unauthorized disclosure occurs

DATA PROTECTION OFFICER

Appoint a Data Protection Officer to oversee implementation of Education Law 2-d responsibilities

DATA SECURITY AND PRIVACY POLICY

Part 121 of the Commissioner's Regulations requires agencies to adopt a policy on data security and privacy by October 1, 2020.[1] Additionally, the law requires agencies to publish the policy on the district's website. To learn more about this requirement, review Part 121.5 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Policy:

✓ Includes All Required Elements

✓ Is Adopted by October 1, 2020

✓ Is Posted on the Agency's Website

✓ Notice is Provided to All Officers and Employees

✓ Third-Party Contracts Require Practices Consistent with the Policy

REQUIRED ELEMENTS

NIST CYBERSECURITY FRAMEWORK ALIGNMENT
Policy must align with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF)

DATA GOVERNANCE
Every use and disclosure of PII by the educational agency must benefit students and the agency

DISCLOSURE AVOIDANCE
Personally identifiable information will not be included in public reports or other documents

PROTECTIONS AFFORDED TO PARENTS
Include all the protections afforded to parents or eligible students, where applicable, under FERPA and IDEA, and the federal regulations implementing such statutes

CONSISTENT WITH STATE AND FEDERAL LAWS
Consistent with applicable state and federal laws

> *POLICIES ARE AVAILABLE THROUGH DISTRICTS' POLICY SERVICES. NYSSBA, ERIE 1 BOCES, AND MADISON-ONEIDA BOCES OFFER POLICY SERVICES TO NEW YORK STATE DISTRICTS.*

[1] The Board of Regents adopted emergency regulations on June 8, 2020. The regulations extended the date required for the adoption and publishing of data security and privacy policies from July 1, 2020 until October 1, 2020.