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

ANNUAL EMPLOYEE TRAINING

Educational agencies are responsible for providing data privacy and security awareness training to their officers and employees with access to personally identifiable information annually. Training should include training on the state and federal laws, and how employees can comply with such laws. Each agency must also provide notice of the agency's data security and privacy policy to all its officers and employees. To learn more about this requirement, agencies can review 121.7 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Training:

- ✓ All Employees and Officers with Access to PII Trained Annually

Specialized Training:

- ✓ Review Section PR.AT of the NIST CSF (Targeted Staff Need Additional Training)

BEST PRACTICES

COMPLYING WITH STATE AND FEDERAL LAWS

Training on the state and federal laws that protect PII, and how employees can comply with such laws.

- **NEW YORK STATE EDUCATION LAW 2-D**
  This law protects the privacy and security of personally identifiable information (PII) of students, and certain APPR data. The law outlines requirements for educational agencies and their contractors.
  - **PROTECTED DATA**
    Employees need to know what types of information are protected.
  - **PARENTS' RIGHTS**
    Employees should be aware of the Bill of Rights. For example, parents have the right to inspect their child's education record.
  - **DISTRICT POLICY**
    Each agency must provide notice of the agency's data security and privacy policy to all its officers and employees.
  - **SECURITY AWARENESS TOPICS**
    The NIST CSF includes controls related to personnel being provided cybersecurity awareness education and trained to perform duties consistent with policies and agreements.
  - **REQUIREMENTS RELATED TO THIRD-PARTY CONTRACTOR**
    Employees must be informed that contracts created through clicking an "accept" agreement are subject to Ed Law 2-d if, as a result of using that contractor's product, the contractor receives protected PII from the agency.
  - **INCIDENT PROCEDURES**
    Employees must be informed of incident complaint, response, and notification requirements.
- **FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)**
  This is the foundational federal law related to the privacy of students' educational records. FERPA limits access to student records and details rules to follow when providing access to or disclosing the data.
- **CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)**
  COPPA imposes requirements on operators of websites, games, apps or online services directed to children under 13, and on online service providers that collect PII online from a child under 13.
- **PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA)**
  PPRA defines the rules states and districts must follow when administering surveys, analysis, and evaluations funded by the US Department of Education.