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

INCIDENT REPORTING AND NOTIFICATION

Educational agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer and notify impacted stakeholders. To learn more about this requirement, agencies can review Part 121.10 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Incident Response Procedures:

- ✓ Outlines All Required Actions

Contracts:

- ✓ Outline All Third-Party Contractor Requirements

REPORTING REQUIREMENTS

10 DAYS TO REPORT TO NYSED
The agency must report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer no more than 10 calendar days after such discovery.

NOTIFICATION REQUIREMENTS

60 DAYS TO NOTIFY AFFECTED INDIVIDUALS
The agency must notify affected parents, eligible students, teachers and/or principals no more than 60 calendar days after the discovery of a breach or unauthorized release.

LAW ENFORCEMENT OR VULNERABILITY DELAY
Where notification is delayed, the agency must notify affected individuals within 7 calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

THIRD-PARTY REIMBURSEMENT REQUIREMENT
Where a breach or unauthorized release is attributed to a third-party contractor, the contractor must pay for or reimburse the agency for the full cost of notification.

METHOD OF NOTIFICATION
Notification must be directly provided to the affected individuals by first-class mail to their last known address; by email; or by telephone.

CONTENTS OF NOTIFICATION
Notifications must be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

- a brief description of the unauthorized release
- the dates of the incident and date of discovery
- a description of the types of PII affected
- the number of records affected
- a brief description of the agency's investigation
- contact information for representatives who can assist parents

MODEL IMPROPER DISCLOSURE NOTIFICATION

This letter is to inform you of an incident that occurred within the [insert system]. This incident resulted in student/staff/etc data being accessed without authorization by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation.

[insert required elements:

- a brief description of the breach or unauthorized release
- the dates of the incident and the date of discovery
- a description of the types of personally identifiable information affected
- an estimate of the number of records affected
- a brief description of the educational agency's investigation or plan to investigate]

Please know that our district is committed to protecting and securing educational data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your child's educational records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident occurring in the future. Please contact [insert name] with any questions you may have regarding this incident and our response [Note: The regulations require agencies to include contact information for representatives who can assist parents].

MODEL UNAUTHORIZED RELEASE COMPLAINTS RECORD

The agency must maintain a record of all complaints and their disposition in accordance with applicable data retention policies, including ED-1. Insert information about complaints into the log.

COMPLAINANT NAME	DATE COMPLAINT SUBMITTED
DESCRIPTION OF THE COMPLAINT	
FINDINGS	
DATE THE FINDING REPORT WAS SHARED WITH COMPLAINANT	