

Regulation 1300-R

Security Breach and Notification Regulation

Approved Upon Superintendent's Initials

Date

1/22/26

I. Purpose

This regulation implements **Policy 1300 – Security Breach and Notification** by establishing procedures to:

1. Identify any breaches of security that result in the release of private information;
2. Ensure ongoing information technology security awareness training for all District employees; and
3. Require prompt notification to the **Chief Communications Officer**, who is responsible for notifying affected individuals in accordance with law and policy.

II. Definitions

- **Breach of security:** Unauthorized acquisition, access, use, or disclosure of private information that compromises its confidentiality, integrity, or availability.
- **Private information:** As defined in Policy 1300 and New York State law (including, but not limited to, Social Security numbers, financial account information, driver's license numbers, and student and personnel data protected by Education Law §2-d).
- **Affected individuals:** Persons whose private information was released or reasonably believed to have been released.
- **Data Protection/Privacy Officer:** The District staff member(s) designated by the Board or Superintendent to oversee information security and incident response.

See Policy 1300 and Section VII below for related definitions.

III. Identification and Reporting of Breaches

1. **Employee duty to report:** All employees must immediately report any suspected or confirmed breach of security involving private information to their immediate Supervisor and/or the Data Protection/Privacy Officer or designee. Reports shall be made no later than **24 hours after discovery**. An employee who encounters

breached data and does not report to a Supervisor, Data Protection/Privacy Officer or Superintendent, and knowingly shares with third-parties who do not have a need to know, could be in violation of district policy and applicable laws, and as such subject to discipline and/or other legal penalties.

2. **Investigation:** The Data Protection/Privacy Officer shall promptly investigate, document, and determine the nature, scope, and severity of the breach.
3. **Internal notification:** If a breach is confirmed or reasonably suspected, the Data Protection/Privacy Officer shall notify the **Superintendent** and the **Chief Communications Officer** without delay.
4. **Documentation:** All breach reports, investigations, and remedial actions shall be recorded and maintained for **six (6) years**.

IV. Employee Training

1. **Initial training:** All new employees shall complete information technology security awareness training at the time of hire.
2. **Ongoing training:** All employees must complete **annual refresher training**, covering:
 - Proper handling of private information;
 - Recognizing and avoiding phishing and social engineering;
 - Secure password/access management;
 - Incident and breach reporting procedures; and
 - District policies on privacy, data security, and breach response.
3. **Updates:** The Data Protection/Privacy Officer will review training materials at least every two years, or sooner if required by new threats or legal requirements.
4. **Compliance:** Completion of training is mandatory. Failure to comply may result in suspension of system access and/or disciplinary action as warranted.

V. Notification of Affected Individuals

1. **Responsibility:** The **Chief Communications Officer** is the official responsible for issuing notifications to affected individuals, in consultation with the Data Protection/Privacy Officer, Superintendent, and legal counsel as appropriate.

2. **Timing:** Notifications shall be made **without unreasonable delay**, consistent with Policy 1300 and state law.
3. **Content:** Notifications shall include:
 - A general description of the incident;
 - The type(s) of private information involved;
 - Steps taken by the District to contain and remediate the breach;
 - Recommended protective measures for affected individuals; and
 - Contact information for District assistance.
4. **Method:** Notice may be given in writing, electronically, or by substitute notice as permitted by law. Where required, state and federal regulators and consumer reporting agencies will also be notified.

VI. Oversight and Accountability

- The **Superintendent or designee** shall ensure resources are allocated to implement this regulation.
- The **Data Protection/Privacy Officer** shall prepare an **annual report** summarizing breach incidents and employee training compliance, to be reviewed by the Superintendent and Board of Education.
- This regulation shall be reviewed **every three (3) years** or sooner if required by changes in law or District policy.

VII. Cross References

- **Policy 1300 – Security Breach and Notification**
- **Education Law §2-d** (student and personnel data privacy and security)
- **General Business Law §§ 899-aa, 899-bb** (New York State breach notification laws)
- **8 NYCRR Part 121** (student data privacy regulations)

Adopted: January, 22, 2026