Central Islip Union Free School District

Board of Education & School District Policy Book
50 Wheeler Rd. | Central Islip | N.Y. | 11722
(631) 348-5000
https://www.centralislip.k12.ny.us

Section	Section Title	Type
8000	Support Services	Regulation
Policy	**Policy Title**	
8635-R	Information Security Breach and Notification Regulation	

This regulation addresses information and data privacy, security, breach and notification requirements for student and teacher/principal personally identifiable information under Education Law §2-d, as well as private information under State Technology Law §208.
The district will inventory its computer programs and electronic files to determine the types of information that is maintained or used by the district, and review the safeguards in effect to secure and protect that information.

Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d

1. Definitions

"Biometric record," as applied to student PII, means one or more measurable biological or behavioral characteristics that can be used for automated recognition of person, which includes fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.
"Breach" means the unauthorized acquisition, access, use, or disclosure of student PII and/or teacher or principal PII by or to a person not authorized to acquire, access, use, or receive the student and/or teacher or principal PII.
"Disclose" or Disclosure mean to permit access to, or the release, transfer, or other communication of PII by any means, including oral, written, or electronic, whether intended or unintended.
"Personally Identifiable Information" (PII) as applied to students means the following information for district students:

1. the student's name;
2. the name of the student's parent or other family members;
3. the address of the student or student's family;
4. a personal identifier, such as the student's social security number, student number, or biometric record;
5. other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does

not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

7. information requested by a person who the district reasonably believes knows the identity of the student to whom the education record relates.

"Personally Identifiable Information" (PII) as applied to teachers and principals means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

"Third-Party Contractor" means any person or entity, other than an educational agency (i.e., a school, school district, BOCES or State Education Department), that receives student or teacher/principal PII from the educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This includes an educational partnership organization that and receives student and/or teacher/principal PII from a school district to carry out its responsibilities pursuant to Education Law §211-e (for persistently lowest-achieving schools or schools under registration review) and is not an educational agency. This also includes a not-for-profit corporation or other nonprofit organization, other than an educational agency.

Complaints of Breaches or Unauthorized Releases of PII

If a parent/guardian. eligible student, teacher, principal or other district employee believes or has evidence that student or teacher/principal PII has been breached or released without authorization, they must submit this complaint in writing to the district. Complaints may be received by the Data Privacy Officer, but may also be received by any district employee, who must immediately notify the Data Privacy Officer. This complaint process will be communicated to parents, eligible students, teachers, principals, and other district employees.

The district will acknowledge receipt of complaints promptly, commence an investigation, and take the necessary precautions to protect personally identifiable information.

Following its investigation of the complaint, the district will provide the individual who filed a complaint with its findings within a reasonable period of time. This period of time will be no more than 60 calendar days from the receipt of the complaint.

If the district requires additional time, or if the response may compromise security or impede a law enforcement investigation, the district will provide individual who filed a complaint with a written explanation that includes the approximate date when the district will respond to the complaint.

The district will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.

Notification of Student and Teacher/Principal PII Breaches

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the Data Privacy Officer in the most expedient way possible, without unreasonable delay, but no more than seven calendar days after the breach's discovery.

The Data Privacy Officer will then notify the State Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party

contractor's notification using a form or format prescribed by the State Education Department.
The Data Privacy Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.
The district will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.
However, if notification would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by disclosing an unfixed security vulnerability, the district will notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.
Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

- a brief description of the breach or unauthorized release,
- the dates of the incident and the date of discovery, if known;
- a description of the types of PII affected;
- an estimate of the number of records affected;
- a brief description of the district's investigation or plan to investigate; and
- contact information for representatives who can assist parents or eligible students with additional questions.

Notification must be directly provided to the affected parent, eligible student, teacher or principal by first-class mail to their last known address; by email; or by telephone.
The unauthorized acquisition of student social security numbers, student ID numbers, or biometric records, when in combination with personal information such as names or other identifiers, may also constitute a breach under State Technology Law §208 if the information is not encrypted, and the acquisition compromises the security, confidentiality, or integrity of personal information maintained by the district. In that event, the district is not required to notify affected people twice, but must follow the procedures to notify state agencies under State Technology Law §208 outlined in section II of this regulation.

"Private Information" under State Technology Law §208

1. Definitions

"**Private information**" consisting of any personal information (i.e., information such as name, number, symbol, mark or other identifier which can be used to identify a person) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

a. social security number; or
b. driver's license number or non-driver identification card number; or
c. account number, credit or debit card number, in combination with any required security code, access code, password or other information, which would permit access to an individual's financial account; or

d. account number or credit or debit card number, if that number could be used to access a person's financial account without other information such as a password or code; or
e. biometric information (data generated by electronic measurements of a person's physical characteristics, such as fingerprint, voice print, or retina or iris image) used to authenticate or ascertain a person's identity; or
f. a user name or email address, along with a password, or security question and answer, that would permit access to an online account.

"**Private information**" does not include information that can lawfully be made available to the general public pursuant to state or federal law or regulation.

"**Breach of the security of the system**" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district. Good faith acquisition of personal information by an officer or employee or agent of the district for the purposes of the district is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

To successfully implement this policy, the district shall inventory its computer programs and electronic files to determine the types of personal, private information that is maintained or used by the district, and review the safeguards in effect to secure and protect that information.

Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the district shall consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts, opened or instances of identity theft reported; and/or
4. any other factors which the district shall deem appropriate and relevant to such determination.

Security Breaches – Procedures and Methods for Notification

Once it has been determined that a security breach has occurred, the following steps shall be taken:

1. If the breach involved computerized data owned or licensed by the district, the district shall notify those New York State residents whose private information was, or is reasonably believed to have been accessed or acquired by a person without valid authorization. The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the integrity of the system.
2. The district shall consult with the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures.

3. If the breach involved computer data maintained by the district, the district shall notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been acquired by a person without valid authorization.

Note: The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after the law enforcement agency determines that such notification does not compromise the investigation.

The required notice shall include (a) district contact information, (b) a description of the categories information that were or are reasonably believed to have been accessed or acquired without authorization and (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) the telephone number and website of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention. This notice shall be directly provided to the affected individuals by either:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the district keeps a log of each such electronic notification. In no case, however, shall the district require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.
3. Telephone notification, provided that the district keeps a log of each such telephone notification.

However, if the district can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the district does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the district has such address for the affected individual;
2. Conspicuous posting on the district's website, if they maintain one; and
3. Notification to major media

However, the district is not required to notify individuals if the breach was inadvertently made by individuals authorized to access the information, and the district reasonably determines the breach will not result in misuse of the information, or financial or emotional harm to the affected persons. The district will document its determination in writing and maintain it for at least five years, and will send it to the State Attorney General within ten days of making the determination.

Additionally, if the district has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act, the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, or New York State Education Law §2-d,it is not required to notify them again. Notification to state and other agencies is still required.

Notification of State and Other Entities

Once notice has been made to affected New York State residents, the district shall notify the State Attorney General, the State Department of State, and the State Office of Information Technology Services, the Consumer Protection Board, and the State Office of

Cyber Security and Critical Infrastructure Coordination as to the timing, content, and distribution of the notices and approximate number of affected persons.
If more than 5,000 New York State residents are to be notified at one time, the district shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.
If the district is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, it will also notify the State Attorney General within five business days of notifying the Secretary.

November 14, 2011
Modified: October 13, 2020