Book	Policy Manual
Section	4000- Instruction
Title	Acceptable Use of School District Computers
Number	4526
Status	Active
Legal	Reviewed by Counsel December 4, 2014
Adopted	December 18, 2014

The Board of Education is committed to optimizing student learning and teaching. The Board of Education considers student access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer related technology in School District classrooms for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

All users of the School District's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The School District reserves the right to control access to the Internet for all users of its computers and network. The School District may either allow or prohibit certain kinds of online activity, or access to specific websites.

Regulations and handbooks, to be developed by the Superintendent of Schools, in consultation with the administrative staff will provide specific guidance on this, as well as rules governing the use and security of the School District's computer network. All users of the School District's computer network and equipment shall comply with this policy and regulation. Failure to comply may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

The Superintendent of Schools shall be responsible for designating an individual(s) to oversee the use of School District computer resources. Said individual(s) will prepare in-service programs for the training and development of School District staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Superintendent of Schools, working in conjunction with the designated purchasing agent for the School District, the individual(s) assigned to oversee the use of School District computer resources and the instructional materials planning committee, will be responsible for the purchase and distribution of computer software and hardware throughout the School District's schools. They shall prepare and submit for the Board of Education's approval a comprehensive multi year technology plan which shall be revised as necessary to reflect changing technology and/or School District needs.

The following rules and regulations govern the use of the School District's computer network system and access to the Internet.

1. Administration

a. The individual(s) designated by the Superintendent of Schools, shall:

- oversee the School District's computer network;

- monitor and examine all network activities, as appropriate, to ensure proper use of the system;
- be responsible for disseminating and interpreting Board of Education and School District policy and regulations governing use of the School District's network at the building level with all network users;
- provide employee training for proper use of the network and will ensure that staff supervising students using the School District's network provide similar training to their students, including providing copies of Board of Education and School District policy and regulations governing use of the School District's network; and
- ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.

b. All student agreements to abide by Board of Education and School District policy and regulations and parental consent forms shall be kept on file in the School District office.

2. Acceptable Use and Conduct

a. All network users will be issued a login name and password. Passwords must be changed periodically.

b. Only those network users with written permission from the principal or individual(s) assigned by the Superintendent of Schools may access the School District's system from off site (e.g., from home).

c. All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are not appropriate.

d. Network users identifying a security problem on the School District's network must notify the appropriate teacher, administrator or Director of Technology. Under no circumstance should the user demonstrate the problem to anyone other than to the School District official or employee being notified.

e. Any network user identified as a security risk or having a history of violations of the School District computer use guidelines may be denied access to the School District's network.

3. Account Access to Network, E-Mail Accounts and Computer Services

a. All student users of the network or computer services may access resources according to his/her assigned rights, with appropriate authorization and parent consent in writing. Approved class work shall have priority over other uses. No single user is allowed to monopolize a computer, unless specifically assigned for special needs.

b. All use of the network or other on-line servers must be in support of education and research consistent with the goals of the School District. The term “education” includes use of the system for classroom, professional or career development activities.

c. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to access their accounts. Users will be held responsible for any policy violations that are traced to their accounts. Under no conditions shall a user provide his/her password to another person.

d. Users may be required to remove files if total system storage space becomes low.

e. Electronic files stored on the school computers may be reviewed by school personnel at any time.

f. The use of “chat rooms” for purposes other than education is strictly forbidden.

g. Students will be allowed Internet access only during instructional time in a controlled environment. A staff member will be required to monitor all of these activities.

4. System Security

a. Software shall be installed by authorized School District computer administration personnel only.

b. The permission of the Director of Technology and Information Systems or the Director of Information Management is necessary in order to download or install software.

c. Permission of the Director of Technology and Information Systems or the Director of Information Management is required for relocation, removal or adjustment of any hardware and/or peripheral device.

d. Food and/or drink shall not be placed in the immediate area where computers are located.

e. Use of personal equipment including, but not limited to printers, scanners, wireless access points (WAP), and switches, is forbidden without special permission from the Director of Technology or the Director of Information Management.

5. Plagiarism and Copyright Infringement

a. Any software that is protected under copyright laws will not be loaded onto or transmitted via the network or other on-line servers without the prior written consent of the copyright holder.

b. Users will honor all copyright rules and not plagiarize or use copyrighted information without permission. Plagiarism is the use of writings or ideas of others and presenting them as if they were the creation of the presenter.

c. The School District will receive written permission from parents and/or guardians prior to publishing any student's work on the Internet or School District web pages.

6. Prohibited Activities

a. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

b. Attempts to log on through another person's account or to access another person's files are illegal and this conduct shall not be engaged in, except that the School District's administrators shall have the right to log on through another person's account and access another person's files for network security reasons or other reasons within their discretion.

c. Any use of the Internet or network for profit is prohibited.

d. Any use of the Internet or network software for a purpose or effect that is deemed by the supervising staff member and/or school administration to be dangerous, objectionable, pornographic, distracting to education, or otherwise offensive in nature is prohibited.

e. Users will not post chain letters or send messages to large numbers of people.

f. Electronic hate mail, harassment, discriminatory remarks, inappropriate language and other illegal and/or antisocial behaviors are prohibited.

g. Users of the network shall only use their assigned passwords and not seek to misrepresent themselves as other users.

h. Users may not use the School District system to engage in any illegal act, such as arranging for a drug sale, purchasing alcohol, engaging in criminal activity, threatening the safety of a person, etc.

i. Unauthorized exploration of the Network Operating System or unauthorized changes to any installed software is strictly prohibited.

j. Student Internet access may be restricted depending on the grade level. All users will be prohibited from accessing social networking sites; playing online games; using personal email services; and watching videos online (unless authorized for a school purpose).

7. Personal Use

a. Users may not use the School District system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use.

b. Users may not use the system for political lobbying in support of or opposition to individual candidates or political parties.

c. Users may not post personal information about themselves or others, such as their last name, home address, work address, phone number, school name or address.

d. Users will not transmit pictures of themselves or others.

8. Personal Safety Restrictions for Students

a. Users will, as soon as practical, disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

b. Users will not meet with strangers they have met on line.

9. Respect for Privacy

a. Users are not to intentionally seek information about other users that could be private in nature.

b. Users will not post private information about another person.

c. Users of the network are not to intentionally seek information about other users that could be private in nature.

10. Vandalism

a. Any act of vandalism is strictly prohibited. Vandalism is the malicious attempt to destroy or harm data or equipment.

b. Uploading, creating or spreading computer viruses is considered to be an act of vandalism.

c. Unauthorized tampering or mechanical alternation, including software configurations is considered to be vandalism.

11. Access to Inappropriate Material

a. Users will not utilize the School District system to access material that is profane or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people. For students, a special exception to certain sensitive materials for projects may be made for literature if the purpose of such access is to conduct research and the access is approved by the teacher or administrator.

b. The user should, as soon as practical, disclose any inadvertent access in a manner specified by their school. This will protect them against an allegation that they have intentionally violated this Acceptable Use Policy.

12. Consequences

Use of the School District's computer network is a privilege, not a right. Inappropriate or unacceptable uses of the School District's computer resources may result in the suspension or cancellation of computer privileges, as well as disciplinary, monetary, and/or legal consequences.

13. Implementation

Implementation of the acceptable use policy will be responsibility of the school administration and/or the instructors. Any appeal may be brought to the Superintendent of Schools, whose decision will be final.

14. School District Limitation of Liability

The School District does not warrant in any manner, express or implied, that the functions or the services provided by or through the School District system will be error-free or without defect. The School District

shall not bear any liability for any damage suffered by users including, but not limited to, loss of data or interruption of service. Similarly, the School District shall not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system.

Users of the School District's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided. Further, even though the School District may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the Board of Education and School District policy and regulations.

15. No Privacy Guarantee

Students using the School District's computer network should not expect, nor does the School District guarantee, privacy for electronic mail (e-mail) or any use of the School District's computer network. The School District reserves the right to access and view any material stored on School District equipment or any material used in conjunction with the School District's computer network.

Cross-ref:

0115 Dignity for All Students Act
4526.1 Internet Safety
5300 Code of Conduct
8630 Computer Resources and Data Management
8635 Information Security Breach and Notification

Ref:

Book	Policy Manual
Section	4000- Instruction
Title	Internet Safety
Number	4526.1
Status	Active
Legal	Reviewed by Counsel December 4, 2014
Adopted	December 18, 2014

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of School District computers for access to the Internet and the World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board of Education directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent of Schools or his or her designee.

The Superintendent of Schools or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using School District computers; and restricting student access to materials that are harmful to minors.

In addition, the Board of Education prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent of Schools or his/her designee shall establish and implement procedures that enforce these restrictions.

The individual(s) designated under the School District's policy on the acceptable use of School District computers shall monitor and examine all School District computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the School District's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the School District's policy on the acceptable use of computers and the internet. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

As part of this policy, and the School District's policy on acceptable use of School District computers, the School District shall also provide age-appropriate instruction regarding appropriate online behavior, including:

1. interacting with other individuals on social networking sites and in chat rooms, and
2. cyberbullying awareness and response.

Instruction will be provided even if the School District prohibits students from accessing social networking sites or chat rooms on School District computers.

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of School District computers for access to the Internet and World Wide Web.

I. Definitions

In accordance with the Children's Internet Protection Act:

- Child pornography refers to any visual depiction, including any photograph, film, video, picture or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner than conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
- Harmful to minors means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

II. Blocking and Filtering Measures

- The Superintendent of Schools or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all School District computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.
- The person designated to oversee the School District's computer network shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the School District.
- The person designated to oversee the School District's computer network or his or her designee may disable or relax the School District's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.
- The person designated to oversee the School District's computer network shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The person designated to oversee the School District's computer network shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the School District's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the School District's computer network for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the School District's computer network shall have no expectation of privacy regarding any such materials.
- Except as otherwise authorized under the School District's Computer Network or Acceptable Use Policy, students may use the School District's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.
- Staff supervising students using School District computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized

forms of direct electronic communications in accordance with the School District's Internet Safety Policy and this regulation.
- The person designated to oversee the School District's computer network shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

IV. Training

- The person designated to oversee the School District's computer network shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- The School District shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not be limited to: positive interactions with others online, including on social networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and how to recognize and respond to cyberbullying and other threats.
- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or Worldwide Web are directly related to their course work.
- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. Reporting of Violations

- Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal.
- The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of teachers.

Cross-ref:

0115 Dignity for All Students Act
4526 Acceptable Use of School District Computers
5300 Code of Conduct
8630 Computer Resources and Data Management

Ref:

Children's Internet Protection Act, Public Law No. 106-554
Broadband Data Services Improvement Act/ Protecting Children in the 21st Century Act, Public Law No. 110-385; 47 USC §254(5); 20 USC §6777
Education Law 1701

Book	Policy Manual
Section	8000 - Support Services
Title	Computer Resources and Data Management
Number	8630
Status	Active
Legal	Reviewed by Counsel December 4, 2014
Adopted	December 18, 2014

The Board of Education recognizes that computers are a powerful and valuable education and research tool and as such are an important part of the instructional program. In addition, the School District depends upon computers as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the Board of Education's expectations in regard to these different aspects of the School District's computer resources, and defines guidelines for adult use of School District computer networked equipment, including those that provide access to the Internet

This policy covers all adult users of computers and other technology that may provide access to the Internet and/or other networks within or linked with the School District. Computer networks provide the School District, its personnel and students with unique opportunities for the sharing of knowledge, information and ideas that can positively impact on the instructional and organizational programs. With access to the system comes the responsibility for proper on-line conduct, acceptable use of the network, proper use of copyrighted material, and sanctions for inappropriate use.

General Provisions

The Superintendent of Schools shall be responsible for designating an individual(s) who will oversee the procurement and use of School District computer resources. Said individual will prepare in-service programs for the training and development of district staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas.

All users of the School District's computer resources must understand that use is a privilege, not a right, and that use entails responsibility. Users of the School District's computer network must not expect, nor does the School District guarantee, privacy for electronic mail (e-mail) or any use of the School District's computer network. The School District reserves the right to access and view any material stored on School District equipment or any material used in conjunction with the School District's computer network.

Copyrighted Material

Any software that is protected under the copyright laws or otherwise not authorized by the School District will not be loaded onto/or transmitted via the network or other on-line servers, without the express written permission of the copyright holder or the School District.

Use of the Internet

- All use of the network or other on-line servers must be in support of education and research or administration/management consistent with the goals of the School District.
- Any use of the Internet for private, commercial and political business is prohibited.
- Any use of the Internet for profit is prohibited.

- Any use of the network for information that is deemed by the supervising staff member and/or school administration to be dangerous, objectionable, pornographic, distracting and/or otherwise offensive in nature is prohibited.
- Users of the network are not to intentionally seek information about other users that could be private in nature.
- The malicious use of School District computers is prohibited.
- Electronic hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited.
- Users of the network shall use only the passwords assigned to themselves and not seek to misrepresent themselves as other users.

Unauthorized tampering or mechanical alteration including software configurations will be considered vandalism, which is prohibited and illegal.

Administrative regulations defining consequences of inappropriate network behavior shall be developed and reviewed annually due to the changing nature of technology.

- Appropriate information and consent forms shall be developed and forwarded to staff on an annual basis.
- Appropriate guidelines for record keeping and access shall be implemented.
- Electronic files stored on school computer may be reviewed by school personnel at any time.

Computer Records Management and Financial Network Security

The Board of Education recognizes that since School District data is managed by computer, it is critical to exercise appropriate control over computer records, including financial, personnel and student information, as well as the School District's financial network facilities. The Superintendent of Schools, in conjunction with the Assistant Superintendent for Business and Operations, and such other employees as he/she deems appropriate shall establish procedures governing management of computer records. The procedures will address:

- passwords,
- system administration,
- separation of duties,
- remote access,
- data back-up (including archiving of e-mail),
- record retention, and
- disaster recovery plans.

School District Limitation of Liability

The School District makes no warranties of any kind, express or implied, that the functions or the services provided by or through the School District system will be error-free or without defect. The School District will not be responsible for any damage users may suffer including but not limited to, loss of data or interruptions of service. The School District is not responsible for financial obligations arising through the unauthorized use of the system.

Review and Dissemination

Since computer technology is a rapidly changing area, it is important that this policy be reviewed on an annual basis, or more frequently, by the Board of Education. The regulation governing appropriate computer use will be distributed annually to staff and students and will be included in both employee and student handbooks.

Cross-ref:

2160 School District Officer and Employee Code of Ethics
4526 Acceptable Use of School District Computers
4526.1 Internet Safety
5300 Code of Conduct
8650 School District Compliance with Copyright Law

Book	Policy Manual
Section	8000 - Support Services
Title	Information Security Breach and Notification
Number	8635
Status	Active
Legal	Reviewed by Counsel December 4, 2014
Adopted	December 18, 2014

The Board of Education acknowledges the State's concern regarding the rise in identity theft and the need for prompt notification when security breaches occur. To this end, the Board of Education directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure. For purposes of this policy, "private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

Additionally, pursuant to Labor Law §203-d, the School District will not communicate employee "personal identifying information" to the general public. This includes social security number, home address or telephone number, personal electronic email address, Internet identification name or password, parent's surname prior to marriage, or driver's license number. In addition, the School District will protect employee social security numbers in that such numbers shall not: be publicly posted or displayed, be printed on any ID badge, card or time card, be placed in files with unrestricted access, or be used for occupational licensing purposes. Employees with access to such information shall be notified of these prohibitions and their obligations.

Any breach of the School District's computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the School District shall be promptly reported to the Superintendent of Schools and the Board of Education.

Definitions

"Private information" shall mean 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 acquired:

- Social security number;
- Driver's license number or non-driver identification card number; or
- Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

Note: "Private information" does not include publicly available information that is lawfully 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 School District. Good faith acquisition of personal information by an officer or employee or agent of the School District for the purposes of the School 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 School District shall inventory its computer programs and electronic files to determine the types of personal, private information that is maintained or used by the School 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 School 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 School 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 School District, the School District shall notify those New York State residents whose private information was, or is reasonably believed to have been 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 reasonable integrity of the system.
2. The School 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 School District, the School 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) School District contact information, (b) a description of the categories information that were or are reasonably believed to have been acquired without authorization and (c) which specific elements of personal or private information were or are reasonably believed to have been acquired. 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 School District keeps a log of each such electronic notification. In no case, however, shall the School 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 School District keeps a log of each such telephone notification.

However, if the School 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 School 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 School District has such address for the affected individual;
2. Conspicuous posting on the School District's website, if they maintain one; and
3. Notification to major media.

Notification of State and Other Agencies

Once notice has been made to affected New York State residents, the School District shall notify the State Attorney General, 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 School 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.

Cross-ref:

5500 Student Records
5550 Student Privacy
9160 Personnel Records

Ref:

State Technology Law §§201-208
Labor Law §203-d