3520.1(a)

Business and Non-Instructional Operations

Information Security Breach and Notification ~~– Version #1~~

~~The Board of Education is concerned about the rise in identity theft and the need for prompt notification when security breaches occur. Therefore, the District will take reasonable security measures to guard against the foreseeable loss or exposure of restricted personal information about staff, students, and parents. The District will consider practices concerning physical, technical and administrative safeguards for both paper and electronic records.~~

~~To this end, the Board 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.~~

~~Any breach of the district's computerized data which compromises the security, confidentiality, or integrity of personal information and information pertaining to District security and maintained by the District shall be promptly reported to the Superintendent and the Board of Education. However, good faith acquisition of personal information by an officer or employee or agent of the District for the purposes of the District is not considered a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.~~

Version #2

The District will take reasonable security measures to guard against the foreseeable loss or exposure of restricted personal information about staff, students, and parents. The District will consider practices concerning physical, technical and administrative safeguards for both paper and electronic records.

The Superintendent or his/her designee shall oversee a process to identify the following information to be kept on file in the Central Office:

Business and Non-Instructional Operations

Information Security Breach and Notification – Version #1 (continued)

- What information is considered restricted;
- Where it currently resides;
- How it is protected; and
- Who is responsible for providing each level of security for each piece of restricted information.

Restricted personal information is defined as that information protected under federal or state law (FERPA, HIPAA, FOIA, etc.,). Examples of restricted personal information includes, but is not limited to, social security or other identification number, financial account access information, medical records, computer passwords and security codes. Restricted personal information does not include information that is lawfully made available to the general public pursuant to state or federal law or regulation.

A breach of information security refers to an unauthorized acquisition of data in either electronic or paper format. Good faith acquisition of such information by an employee is not a security breach if the information is not used or is not disclosed to others without authorization.

The District shall consider an incident response plan to provide direction in the event of a suspected information breach. The plan should be reviewed annually by staff designated by the Superintendent.

In determining whether restricted personal information is reasonably believed to have been acquired by a person without valid authorization, appropriate action should be taken after the following have been considered:

1. Indications that the information is in the physical possession and control of an unauthorized person such as, but not limited to, a lost or stolen computer or document, file or other record containing personal information;
2. Indications that the information has been downloaded or copied;
3. Indications that the information has been used by an unauthorized person to establish fraudulent accounts or instances of identify theft; and
4. Any other factors that the District deem appropriate and relevant to such a determination.

Notice of a breach of information security should be provided to the individual whose restricted personal information has been acquired by an unauthorized person. Notification will be made in the most expedient time frame possible and without reasonable delay, except when a law enforcement agency advises the District that notification will impede criminal investigation.

Notification should be provided to the individual within three (3) working days of discovery of the breach but no later than thirty (30) working days.

Business and Non-Instructional Operations

Information Security Breach and Notification – Version #1 (continued)

Depending on the number of people to be contacted, notification may be in the form of a face-to-face meeting, telephone call, posting on a web site or sending a written notice to each affected person's home. Notice should include the specific information involved and when known, an estimate of how long it has been exposed, to whom the information has been released and how the breach occurred. In addition, the individual should be advised whether the information remains in the physical possession of an unauthorized person, if it has been downloaded or copied, and/or, if known, whether it was used by an unauthorized person for identity theft or fraud purposes.

NOTE: To successfully implement this policy, it is recommended that districts inventory their 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.

Legal Reference: Connecticut General Statutes
1-19(b)(11) Access to public records. Exempt records.
7-109 Destruction of documents.
10-15b Access of parent or guardians to student's records.
10-209 Records not to be public.
11-8a Retention, destruction and transfer of documents
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.
46b-56 (e) Access to Records of Minors. Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified at 20 U.S.C.1232g.).
Dept. of Education 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g) parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
42 U.S.C. 1320d-1320d-8, P.L. 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA)
65 Fed. Reg. 503 12-50372
65 Fed. Reg. 92462-82829
63 Fed. Reg. 43242-43280
67 Fed. Reg. 53182-53273

Policy adopted:

3520.1(a)

Business and Non-Instructional Operations

Information Security Breach and Notification

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.

"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 District. Good faith acquisition of personal information by an officer, employee, or agent of the District for the purpose 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.

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; or
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.

Business and Non-Instructional Operations

Information Security Breach and Notification (continued)

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 Connecticut 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 reasonable 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. 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.

3. 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 of 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 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.

Once notice has been made to affected Connecticut residents; the District shall notify the State Attorney General.

Regulation approved:

Business and Non-Instructional Operations

Electronic Information Security

The objective of electronic information security is to ensure business continuity and minimize business damage by preventing, controlling and minimizing the impact of security breaches. The purpose of this policy is to protect the _____ Public School system's electronic information resources from threats, whether internal or external, deliberate or accidental. Electronic information resources are defined as all District computer equipment, including any desktop or laptop computers and all hardware owned or leased by the school system; the District's computer network, and any computer software licensed to the District; and stored data. This policy shall apply to all users, whether or not affiliated with the District, of District electronic information resources as well as to all uses of those resources, wherever located.

The School System will maintain access management processes to ensure that appropriate access will be afforded to electronic information resources.

Availability of the electronic information infrastructure is crucial to the continued effectiveness of the _____ Public Schools. The District will develop and implement procedures in accordance with prevailing industry standards and applicable federal and state law to manage environmental, developmental and disaster recovery requirements.

The District will educate all users regarding acceptable use and proper security procedures for electronic information resources.

The District will manage electronic information resources in accordance with applicable federal and state law and regulations, including laws regarding the confidentiality of student and personnel information and access to public records.

(cf. 3520.1 – Information Security Breach and Notification)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.

7-109 Destruction of documents.

10-15b Access of parent or guardians to student's records.

10-209 Records not to be public.

11-8a Retention, destruction and transfer of documents

11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

Business and Non-Instructional Operations

Electronic Information Security

Legal Reference: Connecticut General Statutes (continued)

46b-56 (e) Access to Records of Minors.

Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).

Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified at 20 U.S.C.1232g.).

Dept. of Educ, 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Educ. Provisions Act (20 U.S.C. 1232g) parent and student privacy and other rights with respect to educational records, as amended 11/21/96.

42 U.S.C. 1320d-1320d-8, P.L. 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA)

65 Fed. Reg. 503 12-50372

65 Fed. Reg. 92462-82829

63 Fed. Reg. 43242-43280

67 Fed. Reg. 53 182-53273

Policy adopted: