COMMON GROUND HIGH SCHOOL

School Board Policies, Regulations and Bylaws

P3520.1

Business and Non-Instructional Operations

Information Security Breach and Notification

Protection and Prevention

The District will take reasonable security measures to guard against the foreseeable loss or exposure of personal information that it maintains or possesses.

"Personal information" is defined as an individual's first and last name or first initial and last name; personal mark; or unique biometric or genetic print or image, along with any data element listed below:

- Account number, credit or debit card number, that, in combination with any required security code, access code, or password would permit access to an account;
- Social Security number;
- Taxpayer identification number that incorporates a Social Security number;
- Driver's license number, state identification card number, or other individual identification number issued by any agency;
- Passport number or other identification number issued by the United States Government; or
- Individually identifiable health information as defined in 45 C.F.R. sec. 160.103 except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.

Personal information does not include information that is lawfully made available to the general public pursuant to state or federal law or regulation.

A security breach refers to:

- an unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or is reasonably believed to compromise the security, confidentiality, or integrity of personal information and results in the likelihood of harm to one (1) or more individuals; or
- an unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises or is reasonably believed

Business and Non-Instructional Operations

Information Security Breach and Notification

Protection and Prevention (continued)

to compromise the security, confidentiality, or integrity of personal information and results in the likelihood of harm to one (1) or more individuals.

Security Procedures and Practices

A security breach does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency if the personal information is used for a purpose related to the agency and is not disclosed to others without authorization.

The District shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches.

Once it is determined by the District or the District is notified of a security breach relating to personal information the following shall take place as soon as possible, but within seventy-two (72) hours of the determination:

1. Notify the Connecticut State Police, Attorney General and the Commissioner of Education; and
2. Begin conducting a reasonable and prompt investigation in accordance with the security and breach investigation and practices in accordance with state law.

Notification of Breach

Upon conclusion of the investigation, if it is determined that a security breach has occurred and that misuse of personal information has occurred or is likely to occur, the District shall within forty-eight (48) hours notify the Connecticut State Police, Attorney General, and the Commissioner of Education. Within thirty-five (35) days of providing these notices, the District shall notify all individuals impacted by the security breach. These notices shall be delayed upon written request of a law enforcement agency that the notices would impede an investigation.

Contracts with Nonaffiliated Third Parties - Information Security

Agreements calling for the disclosure of "personal information" to nonaffiliated third parties shall require the third party contracting with the District to follow information breach and security standards at least as stringent as those applicable to the District.

Business and Non-Instructional Operations

Information Security Breach and Notification

Other Private Information

In the case of breach of information made private by law that does not fall within the definition of "personal information", the District may engage in similar investigative, response, or notification activities as provided above. Alternatively, the District may, after reasonable investigation, provide notice 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 unreasonable 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.

Depending on the number of people to be contacted, notification may be in the form of a face-to-face meeting, phone 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 identify theft or fraud purposes.

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)

Business and Non-Instructional Operations

Information Security Breach and Notification

Legal Reference: (continued)
65 Fed. Reg. 503 12-50372
65 Fed. Reg. 92462-82829
63 Fed. Reg. 43242-43280
67 Fed. Reg. 53182-53273

Policy adopted: 9/23/19