

COMPUTER AND DATA SECURITY

The district will implement and maintain practices regarding physical, technical and administrative safeguards for both paper and electronic records. Access to records including computer data stored within all computer systems will be strictly controlled for security.

The computer systems administrator is responsible for maintaining security through procedures developed by the superintendent. These procedures will determine who may have various degrees of access to the system and will state requirements for monitoring the continued proper educational use of the system.

These procedures will also describe:

1. Proper methods of disposal of reports containing confidential or financial information at the end of their use.
2. Methods to ensure system security after change of job status of employees having access to system passwords.
3. Methods to provide backup access in the event of the extended absence of the system administrator.

The Superintendent will direct and monitor a process to identify the following elements of computer and data security:

1. What information is considered restricted.
2. Where it currently resides.
3. How it is protected.
4. Who is responsible for providing each level of security for each type of restricted information.
5. Measures to control or reduce district liability in the event of a breach of security including insurable coverage for costs associated with such a breach.

Employees will promptly report to the Superintendent any breach of the district's computerized data that compromises the security, confidentiality or integrity of personal information maintained by the district. The Superintendent will immediately inform the Board of such a breach of information.

Breaches of Security: The Superintendent shall ensure that the district attempts to provide notice of any system security breach, following discovery, to any person whose unencrypted and un-redacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Such attempts to provide notice shall be made with reasonable promptness, except when a law enforcement agency determines and advises the district in writing that the notification would impede a criminal or civil investigation, or the district must take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system.

Approved: 03/19/2012 Last Reviewed: 03/19/2018 Revised: 03/19/2018

The district will also provide notice of the breach if the encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of security of the encryption, or if the security breach involves a person with access to the encryption key.

Definitions

Breach of system security - unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the district as part of the database of personal information regarding multiple individuals and that the district reasonably believes has caused or will cause loss or injury to any state resident. Good faith acquisition of personal information by an employee or agent of the school district for the purpose of the district is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the district and is not subject to further unauthorized disclosure.

Person - means any natural person, not an entity or company.

Personal information - includes an individual's first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted:

1. Social security number.
2. Driver's license number or state identification card number issued instead of a driver's license.
3. Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

Records - means any material, regardless of its physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed or electromagnetically transmitted. This term does not include publicly available directories containing information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.