Business and Non-Instructional Operations

Information Security Breach and Notification

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

To this end, the Council directs the Executive Director, 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 CREC's computerized data which compromises the security, confidentiality, or integrity of personal information and information pertaining to CREC security and maintained by CREC shall be promptly reported to the Executive Director. However, good faith acquisition of personal information by an officer or employee or agent of CREC for CREC's legitimate business purposes is not considered a breach of the security of the system, provided that the private information is not used, for, or subject to, unauthorized disclosure.

- Secure procedures will be implemented to dispose of private information documents and computer files which contain such information.

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.
Re-codified Chapter 14 (1-213)

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.

Information Security Breach and Notification (continued)

Legal Reference:

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

Connecticut General Statutes (continued)

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.).

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. 1232 g.).

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. 53182-53273

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 CREC. Good faith acquisition of personal information by an officer, employee, or agent of CREC for the purpose of CREC 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, CREC shall consider each of the following:

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;
4. Any other factors which CREC shall deem appropriate and relevant to such determination.

Business and Non-Instructional Operations

Information Security Breach and Notification

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 CREC, CREC shall notify those individuals 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 CREC, CREC 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) CREC 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 any of the following means:

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 CREC keeps a log of each such electronic notification. In no case, however, shall CREC 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 CREC keeps a log of each such telephone notification.

Once notice has been made to affected individuals; CREC shall notify the State Attorney General, as appropriate.

Regulation approved: January 2009