SOCS
Connecting Communities

SOCS Rocks!

Twelve Simple Ways to Secure and Protect Students' Information ©

It can happen in any district, and it happens more often than you realize, confidential student data thought to be safe behind firewalls ends up in the wrong peoples' hands. Data breaches generate anger and turmoil within the community, hardship and difficulty for those whose information was taken and the public's wrath for and loss of confidence in school leaders under whose watch it occurs. Data breaches also cost a fortune to fix. Though it depends on the size of the district and the type of information purloined, **industry experts report the average cost to "make things right" is six million dollars ($6,000,000).**

School data breaches are assumed to be the work of hackers operating outside the system, villains whom school leaders have no control over. But that assumption doesn't jibe with the facts.

Almost eighty percent (80%) of school data breaches are caused by individuals whom school officials have at least nominal control over. Here is the breakdown from several recent studies:

- Seven percent (7%) of data breaches originate from school personnel's failure to shred paper records and/or delete electronic ones;
- Sixteen percent (16%) are caused by disgruntled employees who seek to vent their frustrations on the district;
- Thirty-four percent (34%) arise from staff failure to follow prescribed procedures for handling confidential material or, absent prescribed procedures, devising their own;
- Twenty-one percent (21%) are precipitated by third party agencies whom districts contract with for services, but who have meager security in place to protect students' confidential information.

Let's reiterate that point - almost sixty percent (60%) of student data breaches are caused by school employees and another twenty percent (20%) are caused by third party agencies that

districts contract with. School officials have significant control over the former and at least nominal control over the latter. Perhaps this explains why courts are awarding higher amounts in damages to educational institutions who fail to protect confidential student data?

School officials can decrease the possibility that students' personal and private information will be shanghaied by having policies and procedures in place and making sure staff adhere to them. So here are:

Twelve Simple Ways to Secure and Protect Students' Information.

1. **Your school district should have a board policy stating the importance of protecting and securing students' confidential information. The policy should establish the expectation that employees are to secure those records during the course of the day and when they leave school grounds at the end of their work day and that failure to do so could result in disciplinary action up to and including termination.** Related guidelines should be developed that detail the procedures staff are to follow with regard to said documents and set the expectation that student records are to be maintained in a secure location and routinely audited to make sure all the records can be accounted for. In addition, those records are only to be made available to those with a legitimate educational interest in the child.

2. **Your school district should have a board policy stating whether school district personnel are permitted, or not permitted, to take paper records containing students' personal and private information off school premises**. If your staff are permitted to take paper records off campus, then you need to institute guidelines detailing how employees are to secure and protect of those records (including but not limited to) when they are in transit and in the staff members' homes.

3. **Your school district should have a board policy stating whether school district personnel are permitted to store – either temporarily or long term – students' private and personal information on their personal devices such as laptops, smart phones, iPads, USB drives, etc.** If personnel are permitted to do so, you need to have guidelines in place that state how staff are to secure said information on their personal devices and how they are to delete the information (or destroy the devices) once it is no longer needed. It is also wise to develop a log so the employee (and you) know exactly what information was loaded onto a device in case it is lost or stolen. The district should have a clear and understood procedure in place for reporting a potential breach should any of the drives or devices become lost or unaccounted for.

4. **If your school district provides employees with USB drives or mobile devices to perform their work-related duties, you should have a board policy detailing the use and security of any drives or devices that may hold students' personal and private information.** Whenever possible district-provided USB drives or devices should be encrypted. Staff members should keep a log of the students' personal and private information loaded onto drives or devices and conduct regular audits to determine the location of said drives and devices. The district should have a have clear and understood procedure in place should any of the drives or devices become lost or unaccounted for. The policy should also provide that any district provided device or drive may only be used by the employee for school related purposes.

5. **Your school district should have a board policy prohibiting employees from using their personal e-mail accounts to transmit or store students' private and personal information.**

6. **Your school district should have a board policy mandating that staff report any breach (or potential breach) of students' personal and private information (both paper and electronic records).** The policy should stress that any breach (or potential breach) should be reported immediately to the appropriate administrator and detail the actions that administrator is to take once a report is made to him/her. The policy should note that the inability to find a file, drive or devices that contains students' personal and private information constitutes a "potential breach" and they should never take the position – "it will show up somewhere." When a data breach (or potential data breach) occurs the natural inclination is to inform the individuals effected (or their parents/guardians). However, the Ohio Revised Code provides that data breaches are to be reported to law enforcement first and then law enforcement determines when the victims (or potential victims) will be notified.

7. **If your students' Social Security numbers, Medicaid numbers, and/or health insurance policy numbers are stored in electronic databases, then you should add additional layers of security to protect the information and, as feasible as possible, eliminate any direct or indirect connection to the Internet.** You should also check to see if any non-district personnel/ third party vendors have access to those records and what security measures they have in place to protect your students' information.

8. **Your school district should have a board policy requiring regular audits of access logs to determine if electronic databases containing students' personal and private information have been compromised or improperly obtained.**

9. **Your school district should maintain a record of any privacy and/or data security breaches that occur in the district.** This mandate has been part of federal and state law (since January 1, 2008) and failure to maintain such a log puts school leaders in jeopardy. The

types of breaches that need to be logged include: hacks of databases containing students' personal and private information; employees exceeding authorized access and accessing students' personal and private information improperly; individuals using staff's login credentials to access databases containing students' personal and private information; loss of USB drives or other devices containing students' personal and private information (regardless of whether they are district provided or the individual's property); loss or theft of paper records containing students' personal and private information; and inadvertent web exposure or e-mail exposure of students' personal and private information.

10. **If your school district uses a third party agency (ex. email provider, web hosting company, emergency alert system, pay service entity, etc.) that has access to records that contain students' personal and private information, you should request a copy of the security measures they will used to protect and secure said information.** These documents should be reviewed by your IT Department and other knowledgeable person(s) to determine if they are sufficient to protect said information. If you do not feel the security measures the agency has in place are sufficient, then you should cancel your contract with the provider.

11. **Your school district should have a plans in place to monitor the actions of disgruntled employees and to prevent terminated employees from gaining access to and taking students' personal and private information**. Supervisory staff should regularly audit data logs to determine if disgruntled employees have been exceeding their authorized access to pupil files and/or obtaining students' personal and private information improperly. If said instances have occurred (or are occurring) disciplinary action should be taken. When the decision is made to terminate an employee, the district should initiate a termination protocol which includes: nullifying the individual's computer access codes; collecting keys for buildings, rooms and file cabinets; securing the individual's passwords; auditing any protected records in his/her possession etc. Terminating an employee is not an easy task. Administrators often try to make the event less hostile by assenting to requests made by the person being let go. A case in point, in February 2016, a school employee was given notice on a Friday morning that she was being terminated. She asked her supervisor if she could finish the day, and the supervisor gave her permission. By the time the person left at the end of the day she had sent the names, addresses, social security numbers of 1,100 district employee (along with other information) to her personal email account. It took the police ten days to track her down and secure the information.

12. **Educate. Educate. Educate.** Having policies and procedures protecting students' personal and private data is one thing, dispersing that information to district personnel is another. You need to ensure that district policies and guidelines are incorporated into faculty handbooks and addressed on opening staff day and at staff meetings throughout the year. In addition the district should conduct regular reviews to insure everyone is following the prescribed procedures.

By creating policies and procedures that protect and secure pupils' personal and private information, and ensuring that staff are aware of those protocols and are adhering to them, you will lessen the chances that protected information will end up in the wrong person's hands.

***SOCS Rocks!* is made available to educators by:**

Simplified Online Communications System (SOCS), 1300 O Street, Lincoln, Nebraska 68508.

If you have a comment or question about this article or if you would like to suggest a topic for a future edition, please contact Karen Mullins, SOCS Regional Representative at karenm@fes.org.

SOCS
Connecting Communities

A recognized leader in webhosting, network security and marketing!