The following document is from:

Safe and Responsible Use of the Internet: A Guide for Educators

Nancy E. Willard, M.S., J.D.

Responsible Netizen Institute
474 W 29th Avenue
Eugene, Oregon 97405
541-344-9125
541-344-1481 (fax)
Web Site: http://responsiblenetizen.org
E-mail: info@responsiblenetizen.org

Part II. Safe and Responsible Internet Use Plan

6. Disclosure of Personal Information of Students

CIPA Requirements

The CIPA Internet Safety Plan must address the disclosure of personal information of students.

> (I) IN GENERAL.-- In carrying out its responsibilities under subsection (h), each school ... shall--
>
> (A) adopt and implement an Internet safety policy that addresses--
>
> ...
>
> (iv) unauthorized disclosure, use, and dissemination of personal identification information regarding minors[1].

[1] 47 U.S.C. §254 (I)(1)(A)(iv).

Dimensions of the Issue

There are many ways in which personal identification information of students may be disclosed by the district or by school staff. District policy should address all of the following issues. In addition to the need for the district to comply with the requirements of the Federal Educational Rights and Privacy Act (FERPA)[2], Individuals with Disabilities Education Act (IDEA)[3], the Student Privacy Protection Act[4], and, in many states, state student privacy laws.

It is also important to ensure that leaders the school's parent association, such as the PTA, fully understand the important obligations regarding the protection of student privacy, especially related to issues of posting student personal information online and collaborative relationships with commercial entities that may result in the collection and use of market research data from students. At many schools, the PTA is responsible for the dissemination of a student directory and/or a newsletter. Many PTAs are also establishing their own web sites. While the district may not be directly responsible for the actions of a parent organization, if such actions generate controversy, the district or a school will obviously be implicated.

Application Service Providers and Student Records

Application Service Providers (ASPs) offer schools the ability to manage school data. The software and databases are stored on the computers of the ASP companies and accessed by school staff, students, and parents through the Internet. ASPs allow schools to track student attendance, grades, disciplinary records, homework assignments, and more. ASPs can also generate the kinds of statistical data required under the No Child Left Behind Act.

The kind of data that these ASPs create, store and transmit is considered educational data. School districts must comply with the Federal Educational Rights and Privacy Act, Individuals with Disabilities Education Act, and, in many states, state student privacy laws with respect to this educational data. It is permissible for schools to contract with third parties for data services, but the school is ultimately responsible for ensuring that the requirements of the statutes are met.

Any contract with a vendor such as this must be thoroughly reviewed by the district's school attorney to compliance with these educational data laws. Issues that should be addressed include, but are not limited to:

- Regulation of access to student data, including limitations on who has access and records of access requests.
- Management of directory information.
- Procedures to correct or delete data.
- Requirements of confidentiality, privacy protection, and computer security on the part of the ASP.

[2] 20 U.S.C. §1232(g).
[3] 20 U.S.C. §1400 et seq.
[4] Section 445(b) of the *General Education Provisions Act* (20 U.S.C. 1232h(b)).

- District ownership and access to the data in a transferable format at any time -- especially if the contract is terminated or the company ceases doing business.

- Indemnity or limitations of liability -- the ASP will likely seek limitations of liability, but should not be allowed to do so.

Currently, there are insufficient guidelines to address concerns in this area. For example, in the area of computer security standards, there are no established standards for exactly how secure the ASP systems must be[5].

Disclosure of Student Information on School Web Sites

Actions that school staff or students may take that would intrude upon the privacy of a student include posting the student's name, class work, or a picture of the student on a district or school web site.

Schools have mechanisms that allow for the disclosure of student information in student phone books and in other district publications. Parental consent is required for any disclosure. These mechanisms have been developed in accord with FERPA. Technically, when parents grant permission for the treatment of student personal information as "directory information" under FERPA, such information becomes public record and may be disclosed by the district.

However, it is probable that most parents' perception of "directory information" is in the context of a hard copy student phone book or yearbook. If a district presumes that when a parent approves of the disclosure of such directory information this also gives the district to post such material on the Internet, the district is likely to generate a significant level of controversy, especially among parents of elementary students. Parents are simply not very comfortable with this level of disclosure of information about their children on the Internet. Therefore, regardless of what FERPA allows a district to do with directory information, the prudent school district will develop more restrictive regulations related to disclosure of student information on the Internet.

Districts should make a specific request of parents related to disclosures of material and information on the district web site. Districts should also demonstrate the same courtesy to staff. There may be some very good reasons for some staff members to wish not to have their identity disclosed online. For example, there may be a staff member who has escaped a domestic violence situation.

Many districts have responding to this issue by requesting parental permission in a manner that allows for many options, presented in a checklist fashion. Options frequently include: student initials, student first name and last initial, student full name, photo or video of student in group without identification, photo or video with identification, class work without identification, class work with identification, etc. The problem with this approach is it is unworkable. School staff cannot be expected to keep track of this vast amount of individualized information for each

---

An excellent discussion of these issues is found in: McGuire, M. (2000) *Defining the Privacy Zone.* It is available online at URL: http://www.nsba.org/itte/legalmeeting/PrivacyIssues.pdf.

student. Inevitably, a staff member will mistakenly post something that a parent had specifically disapproved.

A more practical approach is for the district to determine what student information is safe, reasonable, and appropriate in accord with the instructional goals for elementary school students, middle school students, and high school students. This set of school level disclosure standards can then be provided to parents with the only option given being that of approving or disapproving the entire set.

It is recommended that for students in high school there be the ability to disclose full names. It is a bit illogical to have the online school newspaper report such things as "Joe made a touchdown or Mary, Sue, and Matt have received scholarships to the state university." By high school age, students should be well versed in online safety skills, so that such disclosure should not present concerns. Parents who have concerns still have the option of not granting approval.

The following are a set of recommended standards. However, districts will need to review these standards in the context of their own community.

> For students in elementary and middle school, the following standards apply: Students will use a limited student identifier (school-developed identifier, that will disguise the actual name of the student). Group pictures without identification of individual students are permitted. Student work may be posted with the limited student identifier. All student posted work will contain the student's copyright notice using the limited student identifier.
>
> For students in high school, parents may approve either the elementary/middle school standards or the following standards: Students may be identified by their full name. Group or individual pictures of students with student identification are permitted. Student work may be posted with student name. All student posted work will contain the student's copyright notice including the student's name.

There have been some reported incidents where a teacher has independently posted student information, pictures, and/or work on their own personal web site. In one incident that was privately reported to the author, the teacher defended his actions by claiming he had a First Amendment right to post such information. Teachers have no rights to post information about minors without permission of their parent. All teachers should understand this.

Disclosure of Confidential Student Information in Staff E-mail Communications

School staff members are generally well aware of their legal responsibilities related to the protection of confidential student information. Problems can emerge in regard to the protection of such information when staff members communicate with each other via e-mail. E-mail tends to be informal. Its use leads to the same kinds of casual conversations as can occur in the staff break room or via a telephone. During such casual conversations, confidential student information can be disclosed. But with e-mail, there is now a permanent record of confidential student information that can be easily disseminated.

Staff should be reminded of their responsibilities regarding confidential student information and warned of the potential problems that can emerge due to the nature of electronic communication. One strategy to address this concern may be to develop some type of code to identify such information, for example the letters "CSI" could be written into an e-mail message or the subject line as a signifier to the recipient of the importance of treating the message properly. The requirement to include such an indicator would be a constant reminder to both the writer and the recipient of the importance of protecting privacy. All such e-mails should be retained in a manner required under student records retention laws.

Disclosure of Confidential Student Information in Student E-mail Communications

Students may also violate the privacy of other students by including personal information in an e-mail message. It is important to teach students to respect the privacy of others when communicating electronically and understand the harm that they can cause when they fail to do so. A prohibition against the distribution of personal information about other students should be included in the District Internet Use Policy. This issue should be addressed in instruction provided to students and again when the inevitable "teachable moments" arise.

Student Self-disclosure of Personal Information

Students may disclose personal information in electronic messages or on web sites. This issue and recommendations for the kinds of information that should be disclosed in electronic communications was discussed in "Safety and Security of Students When Using Electronic Communications."

Third Party Web Sites and Market Research

Market Profiling and Targeted Advertising

Educators view the presence of the Internet in schools as an opportunity to enhance student learning. Educators might be surprised to find that others are viewing the expansion of the Internet in schools from a different perspective: an increased opportunity for advertisers to reach the students and parents to promote the purchase of products and services.

One company that was offering free computers to schools[6]. This company was collecting market research information from students and targeting students with advertisements based on the market research. The company promoted itself to schools as "champions of student privacy." However in their investment promotion materials, they referred to their ability to "capture the 'eyeballs' and e-wallets of a captive and attractive demographic."

Web sites that seek to have educators require or encourage students to establish individual online accounts present special concerns. These accounts are established using either the students' actual names or user names. If advertising is present on the Web site it is likely that the account will be used by the dot.com company to develop an individualized market profile of each

[6] A full discussion of this issue is available in Willard, N. (2000) *Capturing the Eyeballs and E-Wallets of Captive Kids in School*. This report is available online at: URL: http://responsiblenetizen.org/documents/eyeballs.html.

student. This market profile is established by collecting data from and about each individual student as he/she uses the Internet. The market profile enables the company to specifically target advertisements to the specific student based on knowledge of that student's specific demographics and interests. Such activities raise special concerns about student privacy and exploitative marketing activities.

The first place for every educator to look when evaluating a web site is the Web site's privacy policy. Virtually all web sites are now providing information about their data collection activities in a Privacy Policy.

Children's Online Privacy Protection Act

In 1998, the U.S. Congress enacted the Children's Online Privacy Protection Act (COPPA), which authorized the Federal Trade Commission (FTC) to develop rules that placing restrictions on companies in soliciting personal information from children under the age of 13. There is more information about the COPPA requirements on the FTC web site[7]. Essentially, COPPA requires that a web site obtain parental permission to collect any personal identification information from children under the age of 13. Unfortunately, rather than reducing the level of profiling and advertising to children, COPPA appears to have established a situation where such activities are considered OK as long as sites have given parents the opportunity to say "no."

On the FTC Kidz Privacy web site in the section for teachers there is more information for teachers about the law. There is also the following statement:

> Whether playing, shopping, studying or just surfing, today's kids are taking advantage of all that the web has to offer. But when it comes to their personal information, who's in charge? The Children's Online Privacy Act, enforced by the Federal Trade Commission, requires commercial website operators to get parental consent before collecting any personal information from kids under 13. *COPPA allows teachers to act on behalf of a parent during school activities online, but does not require them to do so. That is, the law does not require teachers to make decisions about the collection of their students' personal information. Check to see whether your school district has a policy about disclosing student information*[8].

The significant concern created by this language on the FTC web site is that commercial web sites will directly communicate with teachers pointing to the FTC web site as their authority for their position that teachers can grant approval for the web site to collect information from their students. Because the FTC is a federal government agency, teachers may believe that such actions are perfectly appropriate.

Clearly, districts *must* have policies addressing this issue and the restrictions on such approval must be well communicated to all teachers.

[7] URL: http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/index.html.
[8] URL: http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/teachers.htm (emphasis added).

Student Privacy Protection Act

The Student Privacy Protection Act[9] was included in the No Child Left Behind Act. As of the writing of this document, the U.S. Department of Education is in the process of writing regulations for the implementation of this legislation. Up-to-date information can be obtained from the Family Policy Compliance Office (FPCO) in the Department of Education at PPRA@ed.gov.

The Student Privacy Protection Act applies to educational agencies or institutions that receive funds from any program of the Department of Education. The provisions of the law related to the collection of market research data are as follows[10]: Under the law,

- Schools districts are required to develop and adopt policies – in conjunction with parents – regarding the following:

    - The collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling, or otherwise providing the information to others for that purpose.

    - The right of parents to inspect, upon request, any instrument used in the collection of such information.

- School districts must "directly" notify parents of these policies and, at a minimum, shall provide the notice at least annually, at the beginning of the school year. Districts must also notify parents within a reasonable period of time if any substantive change is made to the policies.

- In the notification, the district must offer an opportunity for parents to opt out of (remove their child) from participation in the following activities:

    - Activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information, or otherwise providing that information to others for that purpose.

- In the notification, the district must notify parents the specific or approximate dates during the school year when these activities are scheduled.

The requirements concerning activities involving the collection and disclosure of personal information from students for marketing purposes do not apply to the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions.

[9] Section 445(b) of the *General Education Provisions Act* (20 U.S.C. 1232h(b)).
[10] Other provisions of the law address a range of other surveying or data collection activities.

Given the degree to which commercial web sites are engaging in the collection, disclosure, or use of personal information from students for the purpose of marketing or selling, school districts will need to be very attentive to the manner in which the requirements of this law will be implemented with respect to student use of commercial web sites. This is especially true since most of the market research activities that the commercial web sites are engaged in are essentially invisible.

Parent's Reactions

Districts should seriously consider the reaction of parents if they were to find out that their children's teachers granted permission or encouraged their children to provide personal information or establish an account on a commercial web site that is now developing a market profile of the children and targeting the children with advertising -- all while the children are using the Internet at school.

Regardless of whether the children are under or over 13, it is likely that there would be substantial parent outrage. Clearly, districts MUST have a policy about disclosing student information on commercial web sites -- and that policy should say: "*NO!*" It simply is not OK for educators to encourage or require students to participate on commercial web sites that are profiling their interests for the purpose of advertising to to convince them to purchase products and services.

Recommendations

There may be occasions where the establishment of a student account on a third party site will be solely for the purpose of supporting an educational activity. This kind of a site may also be collecting student use data for the purpose of improving the educational quality of the site. With proper notification to and consent by parents, the establishment of such accounts should be considered acceptable.

Educators must be able to distinguish between web sites that have an exclusive educational purpose and sites that are profiling and advertising. The key feature to consider is the presence of advertising for youth products and services on the site. If there is advertising present and children are required to establish individual accounts, there is a high likelihood that some form of profiling and advertising will be taking place.

The following are recommended standards for addressing these issues:

- There should be no establishment of student accounts on systems unless there is a clear educational purpose, no advertising for consumer products or services is directed at students, and parents have been fully informed and have approved such accounts.

- There should be no collection, analysis, or sale of individual or aggregated student use data for market research purposes for consumer products or services -- period. The Student Privacy Protection Act allows this to occur if there is parental approval. Such activities are totally out-of-line with the duty-of-care that educators should demonstrate towards their students. Essentially, allowing companies to collect information from students results in

selling their privacy for the purpose of promoting their consumption. Such actions should be considered abhorrent to anyone who cares about the well being of children.

- Allowing data collection in carefully controlled situations to support the development of educational products and services should be considered acceptable, if parental notice, with ability to opt out has been provided.

- If any educational data, as defined by FERPA, IDEA, or state laws, is maintained on the third party site, the contract with the third party site should be reviewed for compliance with all such laws.

- Watch for the new regulations from the U.S. Department of Education related to the Student Privacy Protection Act.