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

Although the author has made every effort to ensure the accuracy and completeness of the information contained in this book, the author assumes no responsibilities for inaccuracies or omissions. Although this book discusses legal issues, nothing contained in this book should be interpreted as the provision of legal advice to any individual, district, or other entity.

Part III. Legal Issues – Internet Use in School

5. Public Records

Instructional Stories

District Internet records and employee e-mail and other personal files are public records, subject to retention and disclosure of the state public records laws, the issue should be addressed within the context of the district Policy and Regulations. The following are the tales of one state education network and three districts.

> One state education network was featured in some news articles about its filtering program and the level of denial hits it was reporting. Some anti-filtering advocates seeking to analyze the kinds of denial hits made a public records request for the actual data. The education network denied the request. The denial was appealed to the

appropriate state agency. The state agency ordered the network to provide the records, but then it was found that the network had destroyed the records. The state agency recommended criminal prosecution but the case was not pursued by the local district attorney. The public advocacy group eventually received new data[1].

A school district employee was fixing the computer of the district superintendent and stumbled onto some sexually explicit materials. The school board convened an emergency meeting. The superintendent did not attend but did submit his resignation. Two local newspapers sought access to the computer files. The board denied the request, but did turn the computer over to legal authorities. No criminal charges were filed. The public records question was addressed in an appeal to the state agency. The board argued that the files were confidential personal notes and therefore exempt. The state's public access agency held that a "public record" is any material created, maintained, received or used by a public agency, and generated in any form or medium, including electronically stored data. The electronic record of Internet use stored on the school district's computer hard drive was clearly a public record[2].

The father of a public school student made a public records request for the Internet usage records of all of the students in the school district. It was apparent that the father was seeking data to support objections to the district's policy of not installing filtering/blocking software. The district refused to provide the records. The father took the matter to court. Two key district's arguments were that the provision of records may result in the disclosure of student confidential information and that provision of the records would violate student privacy. The court ruled that since a program could be used to redact student information, confidentiality was not an issue. Further, since students signed an AUP that indicated their use would be monitored, they had no expectation of privacy. The district also noted the excessive amount of data and the costs involved. The court indicated that this was not a matter of concern if the father was willing to pay for the costs. However, the district did have to pay for the father's attorney fees since the district knew or should have known that under state public records laws it should have provided the records[3].

A TV station made a public records request of the Internet usage records of one of the largest public school districts in the state. The district chose not to fight the public records request. It set up a FTP site to allow the station to down load all available records related to the station's request. Internally, the district prepared an information strategy to positively address any potential negative findings. The district also kept track of all of the costs involved in the provision of the public records, and submitted this bill to the TV station, as was allowed under state law. The TV station was not able to find any instances of inappropriate use of the district's Internet system[4].

[1] URL: http://censorware.net/reports/utah/main.html.
[2] URL: http://www.gannett.com/go/newswatch/2000/november/nw1122-4.htm.
[3] URL: http://www.newsbytes.com/news/00/157754.html.
[4] Personal communication with John Adsit, Director of Technology for Jefferson County School District, Colorado. August 2001.

Moral of Stories

Do not waste district resources fighting public records requests. Manage your Internet records with an understanding that such request may come at any time. Let your district's efforts in addressing legitimate concerns speak for themselves.

Issues of Concern

State laws of public records vary from state to state. Therefore this Guide can only address the issue from a general perspective. The two issues that districts should be concerned about related to the retention and disclosure of public records are:

- The massive amount of data that must be stored and the limited capacity of the district to store such data.

- The potential that the disclosure of data will violate the confidentiality/privacy interests of staff or students. State laws would protect such confidentiality/privacy -- but removing such information from the stored public records could present significant problems.

The one issue that districts should not be concerned about is whether or not public disclosure of usage of the district's Internet system will reflect well or badly on the district or individuals within the district. Public accountability is important. Districts must be prepared to provide accurate and helpful information to the public about its strategies to address the legitimate concerns about potential dangers in student use of the Internet, as well as the legitimate concerns that current technology protection measures are unnecessarily blocking student access to appropriate information. Proactive strategies to educate the community and the press are more effective in this regard than reactive strategies.

Public Records Management

Retention and Destruction

Districts should identify what records are required to be retained under state laws and ensure that Internet usage records are retained and destroyed in accord with the provisions of state law. It is probable that districts will find that all staff e-mail files must be retained for a period of time. In many cases, this period of time is one year. But some records may be more important and thus may need to be retained for a longer period of time. Student e-mail files are not considered to be public records. Therefore, the district must organize its files in a way that will allow for the systematic and frequent destruction of student e-mail files, and the retention of staff e-mail files.

Some state public records laws have provisions that allow for the immediate destruction of non-essential records. Districts should request clarification from the state agency responsible for public disclosure regarding whether or not this provision will allow for the destruction of web usage logs. While issues of confidentiality and privacy can generally be handled with technical means, the sheer mass of data involved in the retention of web usage logs will overwhelm most districts.

If the district is not required under state law to retain web usage records, these records should be destroyed on a regular and routine basis. *But* a district should never, ever destroy records after the receipt of a public records request, even if such records are scheduled for routine destruction. Wait until after the public records request matter has been completed to resume the normal destruction schedule. Districts should analyze the manner in which records are retained so that they can easily and inexpensively redact any personal information.

Retention of Web Records for Quality of Use Analysis

Web usage logs are also important sources of data to enable the district to analyze the quality of student use of the Internet. Therefore, it is very important that representative samples of student usage data be analyzed to ascertain the quality of use. Districts should clarify the public records status of any analysis or reports that are completed regarding web usage. It is probable that reports and the data analyzed in regards to the reports will need to be retained for longer periods of time. Ideally, districts will think that it is important to retain small samples of web usage data over the years to allow for research into patterns of student usage of the Internet in schools.

Staff Awareness

Staff should be regularly reminded that the entire contents of their personal files on their computer, as well as their e-mail, would likely be considered to be public records, and thus subject to disclosure. A requirement that all staff use an e-mail signature that includes their name, title, and the district address is a helpful everyday reminder of the public records status of their electronic communications.