

Supreme Court Ruling: Schools must archive eMail

New rules make eMail subject to legal review.

By Corey Murray, Senior Editor, eSchool News

January 1, 2007 - With more school district business being conducted online now than ever before, school technology leaders should know about new rules flowing from a ruling by the U.S. Supreme Court. Experts say the rules--which require schools and other entities to archive eMail, instant messages, and other digital communications written by their employees--could force administrators to rethink eMail storage policies and take stock of existing technologies to ensure compliance.

According to new federal rules that went into effect Dec. 1, schools, businesses, and other organizations are required to keep tabs on all eMail, instant messages (IM), and other digital communications produced by their employees.

The rules, first approved by the U.S. Supreme Court in April, have been widely reported as important for businesses and other for-profit enterprises. But, according to legal experts familiar with the case, the High Court's ruling also applies to public schools and other nonprofit organizations.

The ruling--which states that any entity involved in litigation must be able to produce "electronically stored information" during the discovery process--the process in which opposing sides of a legal dispute must share evidence before trial--could have significant implications for school technology departments, especially in places where technicians routinely copy over backup discs and other information housed on school servers.

In an interview with *eSchool News*, Alvin F. Lindsay, a partner with Hogan & Harts on LLP, said that while the law has always required schools, corporations, and other entities to produce certain kinds of documentation as evidence in the discovery process, the latest ruling is an affirmation that eMail messages and electronic documents are part of that mix.

An expert on issues concerning technology and the law, Lindsay has called prematurely

deleting or copying over eMail documents a matter of "virtual shredding."

Lindsay says the rules will require schools and other organizations to think about how and where they store digital information in advance of potential legal skirmishes. Schools, for example, might want to conduct technology inventories to better understand what types of eMail storage and data backup systems they have in place; establish guidelines for the kinds of information that must be saved and for those that can be deleted; and decide where to store critical data, so the information is easily accessible in the event of a problem, he said.

The new regulations don't constitute any major changes to the law *per se*, Lindsay said, but by noting that electronic communications should be preserved with the same care and diligence as other business-related documents, the High Court ruling forces managers "to recognize this distinction up front," giving schools, businesses, and even individual users an opportunity to be proactive in efforts to secure relevant computer-based information.

Many districts already are working with their staff members to help them understand they should expect limited privacy when using school-owned technology.

"We have a policy that employees need to sign indicating they have no right to consider anything that they do on our network--including our [voice-over-IP system]--as confidential," wrote Marc Liebman, superintendent of the Berryessa Union School District in San Jose, Calif.

But even that isn't enough, explained Lindsay--not anymore.

Though it's important for educators and other school stakeholders to recognize how information that is sent and received on school computers and other devices might be used in litigation, the new rules represent a call to action for schools and other entities to understand how and where personal

Supreme Court Ruling: Schools must archive eMail

New rules make eMail subject to legal review.

By Corey Murray, Senior Editor, eSchool News

communications between employees are stored on the network, he said.

To do that, several corporations--and even some schools--have begun turning to companies that offer solutions for tracking, storing, and searching for eMail communication and other electronic data.

Roger Matus, chief executive officer of Concord, Mass.-based inBoxer Inc., recently told the Associated Press (AP) his company has received a five-fold increase in requests for solutions that streamline the search and retrieval of eMail messages and other electronic information, compared with six months ago.

"Companies used to focus on how they store information," Matus told AP. "Now, they're focusing on how to retrieve it."

For schools and other entities that often require the assistance of legal counsel, the rules also could translate into higher costs, experts say. Not only will organizations need to find a method of cataloging and searching through eMail and IM in the event of a lawsuit; they also might consider investing in technology that helps them filter through digital photos stored on employees' phones and information tucked away on removable memory sticks, among other portable devices.

The ruling no doubt will force some school leaders to reevaluate their digital storage techniques, but it isn't likely to send administrators into a panic, said Mary Kusler, assistant director of government relations for the American Association of School Administrators (AASA).

"This isn't all that new for school districts," said Kusler, who added: "Most schools already operate this way."

Still, it's important for schools to maintain compliance. To do that, Kusler said, the AASA recommends that administrators verify their systems and servers are robust enough to handle the increase in stored information.

Schools also should check with their respective state and local governments and legal counsel to ensure they meet all pre-established requirements for document retention, she said.

John Q. Porter, deputy superintendent of information systems for the Montgomery County Public Schools in Maryland, said his district has long had a policy for storing electronic communications such as eMail in the event of a lawsuit.

"It happens to us frequently, and we do have a process in place," said Porter, whose district keeps all employee-generated eMail messages for at least 10 weeks. Montgomery County also has a software program that enables district IT staff to search through and cull information archived on the network for review in the event of a legal dispute.

To be fair, he said, the district includes disclaimers that appear on every machine and remote eMail interface reminding employees that any information produced by them and distributed over the district's network is the property of the school system.

"Our understanding is that, as long as you have a process in place so this type of information is discoverable in the event of a lawsuit, then that is fine," said Porter.

Where schools are more likely to get burned is if they don't have a policy for saving electronic information and, in the event of a lawsuit, decide suddenly to erase eMail messages or other documents to avoid detection, noted Porter.

"If you were involved in some type of litigation and decided tomorrow to delete eMail," he explained, "now, that would be a problem."

Despite its existing safeguards, Porter said, Montgomery County officials will look closely at the new rules to decide if any upgrades or changes to the school system's policies are necessary.

Supreme Court Ruling: Schools must archive eMail

New rules make eMail subject to legal review.

By Corey Murray, Senior Editor, eSchool News

"I don't think it's going to change anything, but we certainly are going to have our lawyers take a look at it," he said of the ruling.

Unlike Montgomery County, some districts have learned the importance of archiving and saving electronic communications the hard way.

In late 2002, members of the Oshkosh Area School District in Oshkosh, Wis., found themselves thick in controversy after a local newspaper discovered that school board members had been routinely erasing eMail messages sent to them by constituents.

The *Oshkosh Northwestern*, which requested the messages as part of an open-records request for a story it planned to run on district boundary and consolidations plans, said the

eMail correspondence should have been archived--and that deleting it violated the state's open-records laws.

At the time of the controversy, former state Attorney General Jim Doyle, who is now governor of Wisconsin, agreed that the decision by school board members to delete constituents' eMail messages did, in fact, violate state law. For their part, members of the Oshkosh school board at the time told *eSchool News* they were unaware that eMail messages were public records (see story: <http://www.eschoolnews.com/news/showStory.cfm?ArticleID=4161>).

The Supreme Court ruling that went into effect Dec. 1 confirms this policy for all entities subject to a lawsuit.

Tips on handling electronic messages

In response to the problems encountered by Oshkosh, Wis. school board members in late 2002, an attorney for the National School Boards Association said there are a number of precautions school officials nationwide can take to ensure compliance with the law. Those suggestions, listed below, still hold true today.

"Develop a technology-use policy that is reasonable and enforceable.

"Understand that all electronic correspondence, including eMail, is subject to the discovery process, as well as Freedom of Information Act requests from outside parties.

"Instruct board members to keep personal communications separate from school-related business.

"Set up an archival system for school-related eMail that is not unlike the process used for paper-based documents.

"Use backup discs or drives to store information for as long as your state requires under the law.

**first published in eSchool News in Jan. 2003.*