



MEMBER SERVICES

POLICY SERVICES

SCHOOL LAW

GOVERNMENT RELATIONS

BOARD TRAINING

Advanced Search

Quick Links...

Logins...

ILLINOIS SCHOOL BOARD JOURNAL

CURRENT JOURNALS | SUBSCRIBE | ADVERTISING RATES | AUTHOR GUIDELINES

November/December 2008

Tools: [Print](#) | [Email](#)

Keep it or delete it? How to handle e-records

by Steven M. Baule and Darcy L. Kriha

Steven M. Baule is superintendent of Community Unit School District 201 in Westmont, Illinois. Darcy L. Kriha is an attorney with Franczek Sullivan in Chicago.

With the recent federal court ruling that e-mail and other electronic documents need to be retained in the same way as traditional correspondence and memos has come a strong push by technology vendors to sell school districts expensive backup systems to maintain all district e-mail. But, simpler and more effective methods exist for a school district to use in order to comply with the law.

To begin, district personnel need to understand what must be maintained. The court didn't rule that *all* e-mail must be maintained — only electronic documents related to the organization's mission.

Keeping e-mails from the grandmothers of teachers asking about their spring break plans or chatter between two teachers about where to go for happy hour after school on Friday need not be retained. However, employees using the school e-mail for such communication should be reminded that the district's systems are for educational and research purposes only. Staff should use personal accounts for personal communication. The district's acceptable Internet use policy should articulate specifically what types of communication are appropriate for district systems.

The school board should develop and implement an electronic document retention policy either as an additional policy or within the scope of an existing document retention policy, if the board has one. Many boards don't have such retention policies, since state law governs what print records are retained and those records are maintained by a relatively small number of staff.

With nearly every employee involved in electronic record production and retention, a board policy seems a reasonable decision. Each district should develop a policy and/or administrative procedures for electronic document retention, in conjunction with its legal firm. One clear need is to advise employees that if the district is faced with litigation that no document, paper or electronic, that may be relevant to the case be destroyed. Some criteria to use in determining if an e-mail or other

IASB HOME

WHAT IS IASB

EXECUTIVE SEARCHES

STAFF

DIVISIONS

MEMBER DISTRICTS

EVENTS CALENDAR

ANNUAL CONFERENCE

SCHOOL BOARD ELECTIONS

SERVICE ASSOCIATES

SCHOOL ATTORNEYS

SPONSORED PROGRAMS

PARENTS/PUBLIC

NEWS MEDIA/PRESS

BOOKSTORE

PUBLICATIONS

SITE MAP

Illinois Association of School Boards

2921 Baker Drive
Springfield, Illinois
62703-5929
217.528.9688

One Imperial Place

1 East 22nd Street,
Suite 20
Lombard, Illinois
60148
630.629.3776

electronic document is in need of being retained are:

- It includes a student's name.
- It discusses a staff member's conduct or performance.
- It discusses implementation of school rules, procedures or board policy.

When in doubt, retain a copy of the document.

In order to ensure that appropriate e-mails are retained, a school board can take two simple steps.

The first step

Direct the administration, special education case managers and other student service personnel to create a directory or folder within their e-mail system labeled for the school year, e.g. SY2008, SY2009, etc. They should save a copy of any important e-mail within that folder.

As a failsafe, the district should ensure that sent e-mail is retained within the individual's e-mail folder. This provides a second copy of mail sent within the district and provides a copy of mail sent out of the district that may not have been copied into the SY2008 folder. Many e-mail systems will allow the network administrator to retain control of portions of user mail folders. An organization can therefore ensure all sent messages are retained.

Similarly, a number of e-mail archiving solutions instantaneously archive all e-mail inbound or outbound. The problem with such systems is that the vast amount of spam and other e-mail that has no significant value will take up a great deal of space. Similarly, if a district at some point is required to produce their e-mail, such vast amounts of spam will cost the district more to retrieve and sort through.

Some systems allow archiving by filtering key words or phrases. However, unlike a widget company, school district work vocabulary is fairly diverse and it would be difficult to implement a successful filtering program for a district wishing to capture all significant e-mail through such a rule of thumb.

Similarly, within each employee's network user folder, directories or folders can be set up to hold memos, letters, etc., with subfolders labeled for each school year. This will facilitate the retrieval of documents if necessary.

The district shouldn't rely on a system's ability to date documents, because when servers are restored after maintenance, for example, the date created or modified property of files often changes to the date of restoration.

Also consider where electronic documents should be stored. Storing documents on local hard drives or laptops is not a sound practice. Such a process provides a single point of failure (the local hard drive) and relies entirely on end users for backups.

Documents saved to a network folder are backed up daily (assuming a sound backup strategy for the network) and provide for hardware redundancy with multiple drive arrays on most servers. Also, a key individual's computer can be stolen or a laptop lost more easily than stealing a server in most cases. Servers tend to be larger and stored in secure, limited access, areas.

Another key to retrieval is that many disaster recovery and backup systems are essentially still DOS-based programs that will struggle with directory or file names that don't conform to DOS standards. In naming files, refrain from using punctuation or directory and file name combinations that extend beyond 256 total characters. Many an English teachers' documents have been unrecoverable due to the "." that was added into a file name after an abbreviation.

Second step

Once a systemic set of procedures exists for retaining documents, now the district

needs a systemic process for backing up network and mail servers. Servers should be backed up completely at least weekly. Many systems can be set to back up changes each night (incremental backups) as well as conducting a full or complete backup at the end of each week.

Those weekly backups should be maintained for a month. The end of month backup should be retained for six months and the six-month or end-of-semester backups should be retained for perpetuity. Since items like grades, student projects and discipline records tend to be most complete at the end of the semester, the six-month backups will allow IT staff or a consultant to restore the full scope of materials from the semester at any time in the future.

The person responsible for conducting the backups should check each backup to make sure that they are viable. The simplest test is to restore a random file from the tape each day to ensure that the backup completed correctly. Tapes should also be stored in a location away from the servers themselves. One copy of backups should be kept offsite either at another school or district office in case of fire or other building disaster.

When backup systems are updated, it is important to make sure that the old backup media are either updated into a format readable by the new system or that the necessary "old hardware" is retained to access old media formats in the future. One may think back to the last time they came across a 5 ¼ floppy disk and were able to access the files on the disk. Clearly, in the future, such files need to be retrievable.

Putting this type of backup process in place allows for a reliable system of backing up systems for both document retention and disaster recovery. These simple procedures will allow for a district to be both fully compliant with the law and in excellent position to recover, if necessary, from a catastrophic failure of its network.

At the point where a board is involved in litigation or a likelihood of such a suit is brought to its attention, three standards articulated in *Zubulake v. UBS Warburg LLC* apply to document retention. (2004 WL 1620866 (SDNY 2004))

- The board and counsel must issue a *litigation hold* at the outset of litigation or whenever litigation is reasonably anticipated. The litigation hold should be periodically re-issued so that new employees are aware of it, and so that it is fresh in the minds of all employees.
- Counsel should communicate directly with the *key players* in the litigation, i.e., the people identified in a party's initial disclosure and any subsequent supplementation. Because these *key players* are the *employees likely to have relevant information*, it is particularly important that the preservation duty be communicated clearly to them. As with the litigation hold, the key players should be periodically reminded that the preservation duty is still in place.
- Counsel should instruct all employees to produce electronic copies of their relevant active files. The board and counsel must also make sure that all backup media which the party is required to retain are identified and stored in a safe place.

The *Zubulake* decision gives us the "litigation hold" letter that most boards of education receive from their attorneys when a lawsuit is filed or anticipated.

Shortly after that decision, Federal Rule of Civil Procedure 26 was amended, effective December 1, 2006, to require that parties to federal litigation discuss and disclose relevant documents that are "electronically stored." Severe penalties for failure to comply with the rules can result, although a "safe harbor" provision (Rule 37) provides: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

The board must ensure that it has a comprehensive electronic document retention

policy in place, that systemic system-wide backups are being conducted and that those systems are routinely spot checked to make sure they are working effectively.

Editor's note

IASB PRESS subscribers will find that policy 2:250, *Access to District Records*, and its accompanying administrative procedure, 2:250-AP2, *Protocols for Record Preservation and Development of Retention Schedules*, provide a place for boards to begin this conversation with their attorneys.

[Table of Contents](#)



[Click on Banner for More Information](#)

Although the IASB Web site strives to provide accurate and authoritative information, the Illinois Association of School Boards does not guarantee or warrant the accuracy or quality of information contained herein.

Copyright 1999-2008 by the Illinois Association of School Boards. All rights reserved.
[IASB Privacy Policy Statement](#)