

Electronic Record Retention Requirements Under
Civil Discovery Rules and Public Records Laws

January 10, 2008

The Education Cooperative

Rosann DiPietro, Attorney
Long & DiPietro, LLP
175 Derby Street, Unit 17
Hingham, MA 02043
(781)749-0021
rdipietro@long-law.com

With the proliferation of electronic mail as a means of communication among members of the school community, school technology staff are assuming an increasingly prominent role in the design of school record retention practices and compliance with requests for records in connection with issues in litigation. As discussed below, technology personnel should be part of any team involved in determining whether and how electronically stored information will be maintained, archived, searched and, ultimately, discarded.

1. Civil Discovery Rules

a. the duty to produce evidence in discovery

The term “discovery” refers to the pre-trial process by which parties to litigation obtain information, both from each other and from others, to learn more about the facts supporting or refuting legal claims. Discovery includes the production of documents or other things in response to written requests, taking a view of an accident scene, conducting a physical examination of a party claiming personal injury, answering questions in writing under oath (interrogatories), requesting the admission or denial of certain assertions of fact, and taking sworn deposition testimony. Discovery may be conducted not only with respect to a court case, but also in matters before state administrative agencies, such as the Bureau of Special Education Appeals and the Massachusetts Commission Against Discrimination, to name just a couple.

School officials should be aware that court decisions involving discovery disputes have uniformly reflected the principle that electronic communications, like any other form of written communication, are subject to production in discovery. See, e.g., Linnen v. A.H. Robins Co., 10 Mass. L. Rptr. 189, 194 (Super. Ct. 1999)[interpreting analogous Massachusetts Rules of Civil Procedure]. The Federal Rules of Civil Procedure have been amended to reflect the previously accepted notion that electronic records are to be regarded the same way as paper records in terms of their discoverability in litigation. The rule for production of documents and things (Rule 34) now specifically includes “electronically stored information” as a category if items that are subject to production.

Federal Rule 26(a)(1)(B), amended effective December 1, 2006, requires that each party disclose, without waiting for a formal discovery request, a copy of, or a description by

category and location of, all information, including electronically stored information, that it may use to support its claims or defenses.

“Electronically stored information” includes “writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained” and requires the responding party to translate such information, if necessary, into “reasonably usable form.” Federal Rule of Civil Procedure 34(a).

Under Federal Rule 26(b)(2)(B), parties need not provide discovery of electronically stored information from sources that are not reasonably accessible because of undue burden or cost, unless the discovering party establishes good cause for the need for such information. The party asserting undue burden or cost must still identify the sources of information that are not reasonably accessible. Even if a party is excused from searching for and producing records that would be burdensome to produce, the party is not necessarily excused from its obligation to preserve such evidence, discussed below. It should be noted that even if production is unduly burdensome or costly, the court may still require production if the requesting party establishes good cause.

b. The duty to preserve evidence

With the duty to produce evidence in response to discovery requests comes the duty to preserve evidence in anticipation of such requests. A party can actually be sanctioned by a judge or hearing officer for destruction, alteration or loss of evidence that is relevant to a material issue in dispute.

i. the doctrine of spoliation

Under the doctrine of “spoliation of evidence,” a court may impose sanctions for destruction of evidence in civil litigation based on the premise that a party who has negligently or intentionally destroyed, lost or even significantly altered evidence known or reasonably anticipated to be relevant for a pending or reasonably anticipated legal proceeding should be held accountable for unfair prejudice that results to the other party. See e.g., Wiedmann v. The Bradford Group, Inc., 444 Mass. 698 (2005)[Massachusetts case involving loss or destruction of both paper and electronic records]. The amendments to the federal rules, on which the Massachusetts rules are modeled, make it clear that spoliation applies not only to paper documents but specifically to electronically stored information as well.

ii. When does the duty preserve evidence arise?

The federal rules alone impose no duty on any person or entity to preserve records forever. Rather, the duty to preserve evidence generally arises no later than the time at which a defendant receives notice of the suit, or a plaintiff anticipates filing a claim. In some circumstances the duty of a party to preserve evidence arises prior to the time actual notice of a claim is received as where “a litigant or expert knows or reasonably should know that the evidence might be relevant to a possible action.” Kippenham v. Chaulk Services, Inc., 428 Mass 124, 127 (1998) citing Nally v. Volkswagen of Am., Inc., 405

Mass. 191, 197-198 (1989). “The threat of a lawsuit must be sufficiently apparent, however, that a reasonable person in the spoliator's position would realize, at the time of spoliation, the possible importance of the evidence to the resolution of the potential dispute.” Nally v. Volkswagen of Am., Inc., 405 Mass. 191, 197-198 (1989).

In the case of Wiedmann v. The Bradford Group, Inc., 444 Mass. 698 (2005), receipt of a letter from a former employee’s attorney demanding payment of unpaid commissions constituted sufficient notice of a potential lawsuit.

iii. How does a party establish that spoliation has occurred?

In order to obtain relief for spoliation of evidence by an opposing expert or party, the moving party must demonstrate 1) that there was a negligent or intentional loss or destruction of physical evidence (as opposed to some event beyond that party’s control, such as a fire or flood), 2) that the party or expert was aware that there was a potential for litigation, and that the physical evidence was material to that litigation, and 3) that the loss or destruction of the evidence created prejudice to the moving party. See Nally v. Volkswagen of America 405 Mass. 191, 197, 539 N.E.2d 1017 (1989).

Where the moving party has established that missing physical evidence is material to its case or its defense, the court may apply a balancing test to determine the appropriate remedy. The court weighs the culpability of the party or expert to whom the fault is attributed (was it intentional, knowing, grossly negligent or negligent), the materiality of the evidence, and the potential for prejudice. See Carbone v. Checker Taxi Company et al, Superior Court Civil Case # 90-7707E (Suffolk, December 30, 1994) (Garsh, J.).

iv. What are the consequences?

The court has broad discretion in fashioning a spoliation remedy. Fed. R. Civ. P. 37. Sanctions include precluding the party from introducing certain witnesses or evidence, an instruction to the jury that it may infer that the destroyed evidence was unfavorable to the party that destroyed it, and an entry of judgment against the party (although this remedy, being the most severe, is reserved for the most egregious cases).

v. Application to electronically stored information

It is important to note that spoliation may consist not only of deliberate action on the part of a litigant but also inaction. For example, failure to halt the operation of a routine network operation may expose a party to penalties for spoliation. School districts should keep these principles, as well as state requirements for document retention (discussed below), in mind when they set their defaults for periodic and routine backup, archiving and destruction of records that exist in electronic form, including email. The Rules of Civil Procedure do contain a so-called “safe harbor” provision which provides that parties will not face sanctions for good faith deletion and disposition of electronically stored information:

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.

Fed. R. Civ. P. 37(f).

Not much caselaw has developed since this amendment appeared in 2006 to guide us as to what constitutes a good faith operation of an electronic information system. The comments to the 2006 amendment suggest that parties are required to intervene in the routine operation of an information system in order to prevent regularly scheduled purges from destroying information that is relevant to a legal dispute. This requirement may include saving deleted data from being overwritten, or even, in rare cases, suspending operations that allow individual users to edit live documents, as this may alter their embedded data showing the last time a document was edited. The rule speaks of “good faith,” rather than perfection. In order to determine whether a party acted in good faith, the court will consider, among other things, the steps the party took to preserve specific electronically stored information. The term “litigation hold” has arisen of late to describe the protection of specific information from automated or regularly scheduled purges or overwriting. There is little law to guide us as to whether a party, such as a school district, will be held liable for not intervening to suspend default settings that may automatically delete or destroy certain electronic information in situations where litigation has not yet been filed.

The Linnen case, discussed above, involved pending, rather than potential litigation. The plaintiff requested that the defendant produce electronic mail messages and back up tapes. Upon receipt of that request, the defendant did not suspend its automated process whereby back up tapes containing emails were overwritten every ninety days, thereby allowing retrieval of only those emails that were backed up within the past 90 days. Any older emails that were not already produced by the defendant were lost forever. The court found that the defendant was liable for not suspending its automated computer operation. It appears the defendant simply neglected to act rather than taking deliberate action to destroy evidence. This resulted in perhaps inadvertent, but nonetheless culpable, loss of evidence to which the plaintiff was entitled.

It is also no excuse that the person within the defendant company who actually destroyed the relevant piece of evidence had no knowledge of the lawsuit. See, e.g., Testa v. Walmart Stores, Inc., 144 F. 3d 173 (1st Cir. 1998). Two points are worthy of note here. First, in the face of anticipated or actual litigation, school officials, in consultation with their technology directors and attorneys, should consider what, if any electronic information must be preserved from either deliberate or automatic destruction. Secondly, it is imperative that schools not permit individual users to be able to purge records in the first place. Any email sent or received by a public employee or official should be automatically saved to central location even if it deleted from that user’s local folders. This is importantly not only to avoid sanctions for spoliation but also to comply with retention requirements under the public records law, discussed below. The Supervisor of Public Records has recommended that emails of all users be saved to a common file directory.

We understand that, by now, the majority of school districts routinely archive all electronic mail messages, along with their “metadata.” They also routinely make their archive a searchable database which, we believe, is a must not only to enable searches but also to respond without undue burden to discovery requests for information stored electronically. The burden involved in conducting a search may not excuse a school district from undertaking it. In fact, in the case of W.E. Aubuchon Co., Inc. v. Benefirst LLC, 245 F.R.D. 38 (D. Mass 2007), the court noted that the defendant’s records were accessible but the poor indexing system made it burdensome to search them for information relevant to the litigation. Nevertheless, the court ordered the defendant to conduct the search anyway, because the plaintiff satisfied its burden under the rules for establishing “good cause” for the need for such information.

It should be noted that the “undue burden” objection to producing records only shifts the burden to the requesting party to show that good cause exists to obtain the records. The burden does not take the party in possession of the records completely off the hook. Therefore, it makes sense for schools, in order to save time, to make archived records searchable. If, before a particular record’s retention period has expired, the school district either anticipates suing or being sued, a search can now be made of archived records and any search “hits” should be segregated from those headed for permanent destruction. This is referred to as a “litigation hold.” Once an actual lawsuit is pending, the parties may seek permission from the court to destroy or alter electronically stored information.

The same or similar discoverable information may exist simultaneously in electronic and paper form. In response to a request for discovery of electronically stored information, the language of the federal rules (Rule 34), according to our interpretation, permits a responding party to elect to produce hard copies of information stored electronically, if that would be less burdensome. The rule provides that a party may produce information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable. The Massachusetts Rule is worded slightly differently (“a party . . . shall produce [records] as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request”). In addition, a party is not required to produce the same electronically stored information in more than one form. However, the requesting party may specify the form in which it wishes to receive information, e.g. paper or electronic form. The responding party may object, on grounds of burden, to the form of production requested. If no form is specified, the responding party may elect the form in which it produces such information. Rule 45, which concerns subpoenas of non-parties, contains similar provisions.

The question arises as to whether a party that routinely makes paper copies of all electronic documents would face sanctions for the destruction of the electronic form of such information. Our research has revealed no case in our jurisdiction that provides a clear answer. The cautious route, we believe, is for school districts to preserve the record in its original form, whatever that may be. If they wish to discard electronic records after their retention period has expired, and litigation is pending, they should always seek the court’s permission before doing so.

On a related note, the defendant in the case of Bakhtiari v. Lutz, et al., (Case No. 06-3867)(8th Cir. 2007), was not sanctioned for backing up the contents of the email account

of the plaintiff, a former employee, onto two CD's and then the account was automatically deleted by the defendant's automatic systems maintenance. This back up and deletion occurred two months before suit was filed. The court found that appropriate pre-litigation steps were taken to preserve potentially relevant evidence, relying in part on the fact that this occurred pre-suit, undercutting the plaintiff's claim that the defendant's intention was to suppress the truth.

It has yet to be determined whether a litigant may inadvertently walk into an issue by permitting users simply to records that exist "live" on the computer system. The very act of accessing a record could modify its embedded data. The relevance of embedded data may relevant only to the rare case but it should at least be considered. That being said, our research has revealed no court decision in our jurisdiction punishing a litigant for allowing its employees to simply read electronically stored records while litigation was pending, thereby altering the "last accessed" indication. The most cautious route would be to isolate to a portable storage device mirror images of certain potentially relevant records, including their embedded data, and then seeking the court's permission to discard this information.

Similarly, it has yet to be determined whether litigants must preserve in particular cases such user access information as log-in histories, web access "histories" and search terms. Documents in the traditional sense are not being created but a "record of use" is being created. We understand that school districts do not routinely archive such information nor, to our understanding, must they archive this information under the public records law, which is discussed in more detail below. School officials, in consultation with their technology directors and legal counsel, should determine whether such information is uniquely relevant to a particular claim in which they are involved. For example, if an employee is claiming that he or she did not access an inappropriate web site, it may be useful to preserve the web site history. If the employee is claiming that an inappropriate web site was accessed but he or she was not the person using a particular work station, it may be useful to preserve the password enabled log-in history for that work station. It is useful to consider whether individual users should be empowered to delete their web histories, search terms, or the like.

2. Public Records Laws

Schools have dual obligations under civil discovery rules and the public records laws. These obligations overlap but are not identical.

The civil rules require parties to preserve relevant information, while the public records law requires school districts to retain, for varying lengths of time, records "created or maintained by any public employee or official" regardless of their relevance to anything. What is a record under the public records law may not be a record under the rules of civil procedure. If it is a record, the public records law generally requires the retention of the record for a far longer period than the rules of civil procedure ordinarily would, and

without regard to the pendency of litigation. Despite the logistical problem of cataloging, storing and making “search capable” hundreds of thousands of emails each year, the good news is that, because school districts have to retain records for so long, they will rarely find themselves in the situation faced by the corporate defendant in Linnen, which accidentally destroyed records that were only 90 days old, during a lawsuit.

The definition of a public record is exceedingly broad and includes:

. . . all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any officer or employee of any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose . . .

MGL Chapter 4, Section 7, clause 26.

Any record fitting the above definition must be produced to anyone requesting it, unless the record falls within one or more of sixteen current exemptions from disclosure. MGL Chapter 4, Section 7, clause 26(a) through (q). It should be noted that, just because a record may be exempt from disclosure, it is not exempt from the requirement that it be maintained and retained. The Supervisor of Public Records (SPR) is charged with setting the retention period for documents depending on their content. Schedules of retention are posted on the SPR web site, discussed below.

In addition, the SPR has issued a bulletin and advisory opinions to the effect that e-mail messages are subject to disclosure to the same extent that analogous paper records are subject to disclosure under the public records law. In addition, e-mail messages are subject to records retention policies in the same manner as paper documents, that is, based on their content not the medium in which they are created, received or maintained. Readers can find the SPR Advisory Bulletin at the following web page:

<http://www.sec.state.ma.us/arc/arcrmu/rmubul/bull199.htm>

The Supervisor of Public Records recommends that public entities evaluate email messages for their content and make a decision as to the period of time that these documents must be retained, based on that content. This appears to be a task for which most school districts are ill-equipped. The web site for the Secretary of State’s Office also contains the statewide records retention schedule as well as a guide for electronic record-keeping systems. Links to the retention schedules applicable to schools are as follows:

<http://www.sec.state.ma.us/arc/arcrmu/rmurds/rdsmds.htm>

<http://www.sec.state.ma.us/arc/arcrmu/rmuidx.htm>

We are aware of no specific direction from the SPR as to whether “record of access” information, such as when a user viewed a web site, which web sites were viewed, use of

Google or other search tools, search terms entered, or the like, would be subject to retention. Existing guidance can be found by viewing the statewide record retention schedule, available by clicking on the following link:

<http://www.sec.state.ma.us/arc/arcrmu/rmuidx.htm>.

In our opinion, and until further guidance is provided, it is reasonable to conclude that a user's pattern of accessing information is not a "record" within the public records law. To us, such records of access are more closely analogous to the act of reading a book or reviewing paper records.

In addition, aside from email records, we are not aware of specific guidance as to whether metadata associated with records must also be retained.

We understand that the Secretary of State's Office expects to finalize regulations on electronic records by the end of June 2007.

In general any record that a public entity must retain can only be permanently destroyed with the approval of the Supervisor of Public Records. In addition, a record of the deletion of records is a record! Such records of deletion must be kept for ten years.

3. Conclusion and Recommendations

The State Supervisor of Public Records sets retention periods for records depending on their content, not their form. Similarly, the rules of civil procedure require parties to preserve and produce records according to their potential relevance to litigation which, in turn, depends on their content. School districts, on the other hand, typically store electronic records according to their form, rather than their content. This dichotomy presents a challenge to school districts in deciding how they will (1) meet their obligations under the public records laws and (2) avoid civil litigation penalties for inadvertent destruction of relevant information. They may elect either to continue to archive electronic communications without regard to their content, or they can analyze each record for its content and make a decision as to whether it gets purged or archived and, if the latter, for how long. As noted above, because evaluation of each individual email for its corresponding retention period appears to be a significantly burdensome task, it may be easier for school districts simply to retain all emails, regardless of content, for a significantly long time. For example, school districts may elect to send all email communications to archives after a particular length of time has passed since they were last actively accessed. Then they could make the archive a searchable database and cue the archived material for permanent destruction after a significant time period in archive. If litigation ensues, it should become a regular practice of the school district to search archived emails to determine whether any of those records meet certain search criteria related to the litigation. If so, they should be flagged for preservation from permanent destruction when their archive period expires. If the database is searchable, placing a so-called "litigation hold" on the record should not be particularly burdensome, if the search parameters are reasonably drawn.

School districts should also consider whether a litigation hold must include suspension of routine and automatic network operations such as overwriting back up devices or continued access to “live” records.

In the same fashion as for civil discovery, archived emails can be searched in response to a public records request. The school district would still need to examine any emails produced in response to such a search to determine whether they meet any of the sixteen current exemptions to the public records law found at MGL Chapter 4, Section 7, Clause 26(a) through (q).

Many vendors have now begun to offer email archiving services, which even screen out spam and junk mail (for which there is no retention requirement) before the records are sent to archive. Schools may continue, however, to grapple with the retention of other electronically stored information.

Schools may either follow the public procurement procedures found at MGL Chapter 30B, Section 1 et seq., or they may consult state lists for approved vendors that supply the desired products or services. To our knowledge, there is no separate state contract for email archiving services or products as yet.