



E-MAIL ARCHIVING FOR EDUCATION

CALL:

1-800-846-2030

VISIT:

www.mpccorp.com

A Simple Lesson Plan for School Districts on the Impact of the New Federal Rules of Civil Procedure (FRCP)

INTRODUCTION

Today's educators teach under an increasing expectation of legal challenges. The National School Board Association reports that 25% of public schools have faced lawsuits in the past two years.

According to Citizens Against Lawsuit Abuse (CALA), in fiscal years 2002-2005 the Los Angeles Unified School District (LAUSD) alone spent more than \$183 million fighting or settling lawsuits. This money, as reported by CALA, could have purchased over 200,000 laptop computers for students.

In a Harris Poll on "Evaluating Attitudes Toward the Threat of Legal Challenges in Public Schools", it was reported that two-thirds of K12 school principals (65%) worry that decisions they make will be legally challenged. And, over half of these school principals (51%), feel that the threat of legal challenges is increasing. Principals recognize the legal importance of keeping records. An overwhelming 87% of them reported to have "written up" incidents for protection.

An e-mail message can be used to issue a report on an incident. E-mail messages also record important communication between two participants pertaining to a topic that might in the future become a legal issue. By maintaining a searchable archive of messages, you can avoid burdening a school district's already strained IT resources with the added painstaking and time-consuming task of retrieving e-mail evidence from back-up tapes.

If you enter into civil litigation, there is a strong likelihood that you will be required to produce e-mail messages as evidence. In December 2006, new amendments to the Federal Rules of Civil Procedure (FRCP) resulted in a set of rules for the treatment of electronic evidence for any party involved in litigation, including schools and school districts.

More than 50% of litigation cases now include e-mail as evidence, according to the Massachusetts Institute of Technology (MIT). Prior to the new FRCP amendments, there were no rules that explicitly governed the handling of electronic information, despite the growing use of this kind of evidence.

But with the new FRCP amendments, the unique role that Electronically Stored Information (ESI) plays in Federal courts has now been formally recognized in an updated set of responsibilities.

There is considerable uncertainty and confusion about the applicability of the new ESI FRCP rules in school programs. Some school districts have contributed to this confusion by not providing either a clear explanation of the new requirements or an updated strategy for e-mail retention.

Educational institutions are affected by these rules in exactly the same way as other organizations. School Administrators need to be aware of these new rules, preferably long before being forced to by opposing lawyers. This paper simplifies each of the new amendments and explains their relevance to e-mail management. The paper also suggests ways that MailFRAME e-mail archiving can help school administrators reach a state of Discovery Readiness.

While there have been few if any fines levied against educational institutions for ESI infractions so far, the very large penalties that have been recently imposed on corporations when ESI has gone missing, establish precedence for probable future rulings in educational-oriented litigation.

A few facts should be very clear. First, ignorance of the new laws will not be tolerated by the courts, and secondly, the onset of litigation is the worst possible time to begin to address Discovery Readiness and e-mail archiving.

Rule 16 – Addressing electronic evidence

Rule 16 states that both parties are to agree on how to address issues pertaining to the disclosure of ESI, and that this shall be done early in the proceedings. Rule 16 requires that, at the beginning of the Discovery process, the two parties reach agreement on how electronic evidence will be disclosed. Whatever is agreed upon however, is subject to the other amendments explained in this paper.

Relevance to E-mail Retention:

When two parties meet early in the Discovery process to address e-mail and other ESI evidence, if one party can demonstrate that it is able to produce e-mail evidence quickly, and in its original form (regardless of age), it puts great pressure on the other party to comply. This competitive advantage does not guarantee success, but positions you favorably and leaves your opponent on the defensive.

MailFRAME E-mail Archiving:

The MailFRAME model of e-mail archiving automatically captures a copy of every message that passes through a school district’s mail server(s), and stores it as a file, preserving the content and format of the original message.

MailFRAME stores messages as vendor-neutral files in a format called RFC-822, the IETF standard for Internet e-mail. This means that if the school deploys MailFRAME e-mail archiving, any message can be viewed in its native file format while it is still in the archive, or replayed (redelivered) to any SMTP-compatible e-mail system. This process preserves the content and form of the original message, deflecting a possible challenge to the legitimacy of a school’s Chain of Evidence¹.

Because the archive is remotely accessible, you can search and retrieve archived messages directly from any computer with a browser, even one in the lawyer’s office or courtroom (with the appliance installed in your DMZ).

Rule 26 - Early disclosure

Rule 26 explains the responsibility imposed on a party to disclose ESI evidence early in the proceedings.

Even though it is not completely necessary for all related evidence to be produced during Discovery, Rule 26 defines an additional responsibility on each party to identify the sources of that electronic information for which the party feels is impractical to produce, along with an explanation of how the information could be gathered and presented, if requested

Whether all of the evidence is produced or not, Rule 26 clearly outlines a requirement for both parties to disclose early in the proceedings, any and all issues relating to the production of ESI evidence.

Relevance to E-mail Retention:

When a teacher or administrator is sued, the school district may have only 30 days to produce relevant e-mail evidence. The ability to quickly produce messages, and in their original form, demonstrates to the court an unquestionable willingness to provide evidence as requested. A party that can demonstrate that production of e-mail messages—even very old ones—is not onerous or time-consuming is viewed favorably by the court and places considerable pressure on the opposing party.

MailFRAME E-mail Archiving:

Using the MailFRAME web-based Search and Replay™, any e-mail message, even a message many years old, can be quickly identified and produced for the proceedings.

Once again, a high-water mark is established that the other party is pressured to also meet, or risk appearing less diligent and forthcoming by comparison.

Rule 33 - E-mail as an official record

Rule 33 stipulates that a review of evidentiary records must include ESI. This amendment now formalizes what has been known for years—that e-mail messages pertaining to a given transaction have value to a future case, and must be treated with the same safeguarding as other records.

With Rule 33, there is no longer any doubt that evidence requested during a civil suit must include related e-mail messages, even when e-mail content is not explicitly requested. The gathering of records imposed on a party by the court now presumes both physical and electronic records.

Relevance to E-mail Retention:

The ability to quickly retrieve e-mail messages related to a specific transaction is essential when involved in a civil suit. Retrieving e-mails from back-up tapes is an extremely costly and time-consuming process. Most school districts are very limited in available IT resources and would be hard-pressed to absorb this substantial additional workload.

On the other hand, an e-mail archiving system that had been capturing e-mail messages and is able to provide quick and easy retrieval can save hundreds or thousands of hours preparing for Discovery. An archiving system that captures messages automatically is vital. There are many recently publicized examples of how human intervention can lead to human error.

¹The term “Chain of Evidence” refers to a legal challenge to the authenticity of a body of evidence, based on the assumption that the more steps and more people involved in storing and producing evidence, the more likelihood there is of tampering or inadvertent modification.

A Store-it-All approach to e-mail retention has become very popular. This is largely due to the costly penalties that could result from unintentional deletions. Although some organizations attempt to automatically filter out messages that have no obvious record value in order to limit unnecessary storage, there is considerable risk in this approach. Messages that may not appear to have legal significance, could in fact be confirming a decisive agreement between two parties. For example, the legal relevance of an e-mail message from one teacher to another that reads simply: "Yes you free for lunch?" could easily be interpreted as a simple invitation to lunch. An innocuous looking message like this one could however be the teacher responding affirmatively to a serious question from another teacher, such as: "So, you actually saw Billy taking the books out of the library?"

By avoiding having to search through old back-up tapes, where data is not indexed, an archiving system can quickly find e-mail messages dating back many years and save valuable time when evidence is requested.

MailFRAME E-mail Archiving:

The MailFRAME e-mail archiving system automatically captures every message that passes through the schools mail server(s). Messages are stored in the archive as files. Because network file storage technology is very economical, the cost of e-mail storage using MailFRAME is as low as US\$2.00 annually for each user². Attempting to filter-out low-value messages to reduce storage costs will not only have a negligible financial benefit, it will also increase the likelihood of costly accidental deletions.

A request for e-mail evidence is a particularly difficult challenge when those messages were archived or backed up while using a previous messaging system. Back-up tapes cannot easily be restored for mail-servers that have been retired, and many e-mail archiving systems are inextricably linked to an old mail-server application. But because MailFRAME systems are vendor-neutral, retrieving (replaying) archived mail is quick and easy, even when the original mail server has been replaced by a new application.

Since there is no limit on how far back Discovery requests for evidence can go, the MailFRAME ability to easily retrieve even very old messages, independent of which messaging system is currently in place or was being used at the time the message was first captured, can save the school district a great deal of effort, money, and frustration.

MailFRAME offers the facility to search for metadata from specific e-mail messages. A Triangulated Search (using Sender, Recipient and Date as search criteria) is usually completed in just seconds. Searches for words (in the subject or message body) can take longer.

Rule 34 - Form of e-mail evidence

Rule 34 specifies that a requesting party can stipulate the form in which electronic evidence shall be produced. This will usually result in a party specifying that the ESI evidence of the other party be produced in its original form, and not as a representation of the message such as a printout or an image (e.g. TIFF, PDF).

Relevance to E-mail Retention:

The importance of original form is once again tied to Chain of Evidence. Any alteration of the evidence, even just for the purpose of presentation, leaves open the suspicion of evidence tampering.

What is the "original form" of an e-mail message? If messages are received in Outlook, does that suggest that a specific Outlook view of the message is "original form"? This is unlikely since the message might have been sent from a Notes user, or it could have been sent to two recipients, one using Outlook and one using GroupWise.

Future case precedents will likely validate that the most probable "original form" of an e-mail message will be the format that all mail server's support—Simple Mail Transfer Protocol (SMTP). RFC 822, the IETF standard for defining the format of SMTP messages is the most vendor-independent e-mail message format available because it is a standard that is supported by every e-mail server application.

Therefore, to be fully prepared to produce e-mail evidence in its original form and avoid potential challenges to its Chain of Evidence, a school district should be able to both capture messages in a standard RFC 822 format and produce them without alteration.

MailFRAME E-mail Archiving:

With a MailFRAME e-mail archiving solution installed, e-mail messages are captured and stored as RFC 822 files. This means that every message archived by the school is both stored and replayed in "original form".

By storing messages as RFC 822 files, messages can be viewed by a browser, and when required, can be replayed to any designated mailbox through any mail server. The MailFRAME capture and replay process preserves the time, date, and content of the original message.

Because the MailFRAME system stores and replays messages in an original form, the school can avoid Chain of Evidence challenges by producing e-mail evidence through what is effectively a Chain of One Link.

Rule 37 - Safe Harbor

As stated in Rule 26, it is not absolutely necessary that all pertinent electronic evidence be presented during Discovery. Rule 37 provides a participating party with protection from possible sanctions in those situations where information has been misplaced or would be too time-consuming or costly to produce.

² Assumes the cost of network disk file storage is \$5 USD per GB and the Radicati Group's estimate of 4 GB/user/year as the current average e-mail data storage requirement.

This protection, referred to as “Safe Harbor”, is only justified however when “good faith” routine operations can be demonstrated. The definition of good faith remains somewhat obscure. The legal use of the term in corporate law holds business leaders responsible for demonstrating appropriate care and loyalty. This suggests that good faith treatment of ESI acknowledges the importance of ESI as future potential evidence and the implicit need for its preservation.

The typical use of the term “good faith” in corporate law holds parties responsible for demonstrating appropriate care and loyalty. This suggests that good faith treatment of ESI should acknowledge the importance of ESI and treat it as future potential evidence with an implicit need for its preservation.

Relevance to E-mail Retention:

Organizations have for many years found shelter against the exposure of questionable e-mail evidence with a strategy of Hiding the Smoking Gun, the routine deletion of e-mail messages. This approach was commonly recommended by corporate lawyers as a strategy for preventing damaging information from arising under subsequent litigation.

Now that Rule 37 specifies the existence of good faith operations, it is hard to imagine that systematic deletion of potential evidence could ever be considered by Federal courts as exemplifying good faith. As a result, Rule 37 will effectively put an end to the legal tactic of deleting e-mails to Hide the Smoking Gun.

Some school districts may be willing to gamble that, in spite of these new FRCP rules for ESI, the courts will accept their policy of regular e-mail deletion and the difficulty of restoring mail from back-up tapes as justification for Safe Harbor. This is a gamble however that could prove to be very costly.

Schools would be hard pressed to argue that these new rules do not apply to them. For educators, the term “good faith” implies that e-mail records be managed with the same rigor as other school records and assumes that responsible policies and effective systems need to be in place to capture and manage these records.

MailFRAME E-mail Archiving:

A MailFRAME e-mail archiving system establishes an effective and simple good-faith e-mail retention operation, primarily because of the following characteristics of the MailFRAME system:

1. Automatic e-mail capture (at zero-hour)
A message is archived immediately as it is sent or received. This avoids the limitation of some archiving systems that run archiving as a scheduled task and leave open the possibility of missing messages (e.g., when a user sends a message and then immediately deletes it before the next scheduled process is run).
2. Captures and stores messages in their original form (RFC 822)
Messages are stored in a format that is compatible with every mail server, RFC-822. As such, archived messages can be replayed exactly as they were originally sent or received, to any mailbox, using any mail server—all the while retaining the content, format and date/time of the original message.
3. Limited Access for Users
Users can search, view, replay, forward, reply to their own messages in the archive, but only have access to their own messages. Users cannot delete or modify archived messages. Even those with Administrator rights cannot modify messages and can only delete messages through the pruning operation (e.g. messages older than a specified age).
4. Vendor independent
Regardless of the messaging environment or changes made to the messaging environment, the replay process is always direct to the mailbox, thereby ensuring a “Chain of One Link”.

Rule 45 – Subpoenas include ESI

Rule 45 imposes responsibility on a party when subpoenaed, to include ESI in its searches for pertinent information. This is similar in nature to Rule 33 (above), which specifies that searches for relevant records must incorporate ESI.

And as with Rule 34, Rule 45 also states that the subpoena may specify the form in which this electronic evidence is to be produced.

Relevance to E-mail Retention:

Rule 45 states that the subpoena may specify the form of e-mail evidence. However, if the form of e-mail messages is not specified in the subpoena, be aware that anything other than its original form could lead to a challenge of its authenticity (e.g., “Chain of Evidence”).

MailFRAME E-mail Archiving:

As discussed under Rule 33 and Rule 34, the MailFRAME solution automatically captures all mail that passes through the mail server(s), as well as providing the ability to search and find e-mail evidence quickly and easily. Because messages are captured and stored as RFC-822 files, they are available for replay to any mailbox, at any time, in their original form.

SUMMARY

This paper explains the various imperatives for the retention of e-mail messages for educators and school administrators that have been articulated in the December 2006 amendments to the Federal Rules of Civil Procedure (FRCP), specifically addressing Electronically Stored Information (ESI).

There are no unique rules for educational institutions. The ESI rules apply to all parties participating in civil litigation, regardless of type of organization and size.

New ESI FRCP amendments:

- FRCP now includes a responsibility on both parties to come together early in litigation and decide how to deal with ESI (Rule 16).
- Both parties have a responsibility to disclose e-mail evidence early in the proceedings (Rule 26).
- E-mail messages are now formally recognized in civil litigation as official records (Rule 33).
- One party requesting e-mail evidence from another party may specify the form of such evidence (Rule 34).
- A party is provided with Safe Harbor protection when e-mail evidence has been misplaced or is too time-consuming or expensive to produce, but only if routine "good faith" operations can be demonstrated (Rule 37).
- A search for information as a result of a subpoena must include relevant e-mail messages (Rule 45).

A "good faith" routine operation for e-mail retention in school districts should include three tightly related and critical elements:

1. A responsible Policy,
2. A Process which supports that policy, and
3. A System that ensures the consistent application of that process

MailFRAME provides an e-mail archiving solution to help you reach a state of discovery readiness through the simple and effective automation of e-mail retention.

Some highlights of the MailFRAME solution:

- Captures all e-mail automatically at zero-hour
- Stores messages as vendor-neutral RFC 822 files so that retrieval is simple, even when the mail server has been changed
- Search and Replay™ can be performed directly from any computer, even one in a lawyer's office or court-room
- Minimal e-mail storage costs because messages are archived to inexpensive standard network file storage (e.g., NAS, IP SAN)
- Fast and easy retrieval of any message
- Messages replayed in their original form (provides a "Chain of One")
- Archived messages cannot be modified or deleted

ADDENDUM: OVERVIEW OF MAILFRAME E-MAIL ARCHIVING

The MailFRAME is a family of vendor-neutral e-mail archiving appliances that automatically capture a copy of every message that passes through the mail-server. The appliance also provides users with an easy-to-use self-search utility called Search and Replay™, to help them quickly find any archived message.

The MailFRAME uses any standard network file storage system as its archival repository (MailFRAME Archive). Storage can be a NAS or just a network server with a suitable-size hard drive – that is, any storage option that supports CIFS or NFS. Because captured messages are stored as vendor neutral files (RFC822 format) in the MailFRAME Archive, they are compatible with any mail-server that supports SMTP.

At the same time that messages are captured, they are also indexed:

- Header information is stored in the appliance-resident database (a backup of each record is created in real time and written to the network share)
- Message body content is indexed and stored in an inverted index table on the network share
- A Message Map is created for each message and stored in the onboard database. The Message Map is used to render a proper view of the message while it is in its raw RFC822 format

The Search and Replay™ application on the MailFRAME provides users with the ability to search for messages using commonly used search criteria, including words in the Subject Line or words in the Message Body.

After specific messages have been found, Search and Replay™ offers the user a number of useful options:

- View Messages: A message can be viewed while it is still in the archive
- Replay Messages: A user can have one (or many) of their archived messages replayed using the current mail-server to their inbox.
- Stand-in Mail Services™: From the message view, a user can Reply to a message, Forward a message, and even Compose a new message, even when the mail-server is unavailable.

MPC does not warrant or represent that the MailFRAME e-mail appliance will cause or permit the Customer to achieve compliance with the Federal Rules of Civil Procedure, HIPAA, a court-ordered discovery requirement or any other legal or regulatory matter. Customer purchases and uses the MailFRAME at its own risk when using the appliance to attempt to comply with any legal or regulatory mandate, and Customer assumes full responsibility to research and verify that the MailFRAME can satisfy any particular legal or regulatory requirement to which Customer may be subject. The case studies presented herein are by way of example only and may not apply to any Customer's particular facts or situation, AND ALL WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE HEREBY DISCLAIMED. All materials of third-party authorship presented herein are reproduced under license from the author, copyright owner, or both, and MPC disavows both (i) any affiliation with or endorsement by any third-party source and (ii) responsibility for the accuracy of any third-party materials.