



# School Law Practice

## Adopting, Implementing, and Enforcing a Records Management Plan Applicable to Electronic Information

*By: Michael D. Hodge & Thomas A. Mickes, Doster, Mickes, James, Ullom, Benson & Guest, L.L.C., Chesterfield, Missouri*

### Contents

**Article:**

Adopting, Implementing, and Enforcing a Records Management Plan Applicable to Electronic Information ..... 1

**School Law Practice Pointers:**

Key Steps to Successfully Adopting, Implementing, and Enforcing a Records Management Plan ..... 2

**Sample Policy:**

E-mail Records and Electronically Stored Information ..... 4

**Article:**

Implementing a Litigation Hold Applicable to Electronic Information ..... 5

**School Law Practice Pointers:**

Key Steps to Effectively Implement a Litigation Hold ..... 6

**Sample Notices:**

Preservation of Historical Documents ..... 10

Preservation of Current Documents ..... 10

Volume 1, Number 1  
June 2007

With the increasing use of communication based technology in school districts, it is more important than ever that school districts stay ahead of the curve in managing their electronically stored information (ESI). This article discusses the relationship between retaining ESI and the new Federal Rules of Civil Procedure's e-Discovery Rules. This article also discusses how to adopt and implement a plan to effectively manage ESI and other electronic communications tools, such as desktop and laptop computers, network servers, PDAs and cell phones, scanners and copy machines, disks, CDs, DVDs, thumb drives, digital voicemail systems, and backup disks. Practical, day-to-day considerations that should be conveyed to school district employees, including suggestions on how to effectively enforce the plan are also covered.

### Electronically Stored Information, the New e-Discovery Rules, and the Impact on School Districts

The Federal Rules of Civil Procedure have recently gone through a major revision to include new electronic discovery rules with the purpose of directing attorneys to keep up with the electronic advances of the 21<sup>st</sup> century. In simpler terms, ESI is now included as discoverable materials. The immediate response from many school district officials is, "What impact does this have on us?" Unfortunately in today's litigious environment, the inclusion of ESI in the Federal Rules mandates that school districts get their electronically-based communication systems organized in a hurry, lay out a clear management plan, as well as properly educate their staff about their new records management policy provisions and corresponding management plan. Key steps a school district can take to accomplishing these goals are described in the School Law Practice Pointers section on page two of this article.

### ***Now Is the Time to Get Organized***

Some school districts invariably will not get organized until they are actually facing litigation, which poses numerous problems for both the school district and their legal counsel. Because the task of getting organized is often difficult and cumbersome, it tends to slide down the priority list or get shuffled down to someone with less than the appropriate training necessary to properly complete the task.

School districts that are not properly prepared risk losing critical evidence without having a justifiable reason. The failure of having a good faith reason for not being able to produce relevant evidence could result in sanctions being handed down by the court, thus costing the school district unnecessary legal fees as well as money paid in fines for contempt of court. For these reasons, prudence and good management dictate that

every school district have an adequate records management policy and plan in place. Thereafter, continual and regular management and enforcement of the plan must occur.

### ***Assessing Which Electronically Stored Information Should Be Retained***

The Federal Rules mandate that an entity retain documents that are relevant to a claim or defense to a claim, subject to limited exceptions. Making a determination of which ESI documents should be retained is a difficult but necessary endeavor, and must be done in good faith. Ultimately, any ESI document that is relevant must be saved for an extended period of time and should either be printed and physically filed in such a way that the documentation is easily retrievable or saved directly to an electronic file on one of the district computers from which it will be easily retrievable.

Irrelevant ESI documents in the system should be regularly deleted. If they are not and litigation arises, the school district will then be forced to search through a litany of “orphaned” ESI documents that serve no purpose and as a result cost the school district unnecessary time and money.

### ***How to Get Organized: Review Your ESI Policies with e-Discovery in Mind***

First, it is critical to determine what information a school district is currently storing and for how long it is stored. If your client is currently purging ESI documents that may be subject to discovery in litigation, the district may be putting itself at risk for allegations of spoliation. Spoliation is the improper alteration or destruction of documents, including electronic data, which can result in sanctions against a school district, ***even where the loss of the electronic data was done inadvertently.***

Second, it is important to consider from whom information is created and the impetus for the creation of that material. The results of this inquiry will allow the school district to better organize its ESI and more easily explain why the ESI was organized in the manner in which the

### **School Law Practice Pointers**

#### **Key Steps to Successfully Adopting, Implementing, and Enforcing a Records Management Plan**

1. Commit to the task of organizing data.
2. Determine what data currently is being stored and for how long.
3. Determine who is creating what information for what purposes to figure out the best way to organize data and to be prepared to explain why particular data was not retained.
4. Determine which documents need to be retained.
5. Determine a method for retaining documents (printed out and/or saved to an electronic file).
6. Adopt a written records management policy and plan.
7. Educate all employees, particularly those using electronic devices, about their obligations under the records management policy and plan.
8. Evaluate employees' compliance with the records management plan, and hold employees accountable if they have not complied with it.

district determined was most appropriate for its purposes. Thus, if something is discarded, the school district will know why and will be able to present that rationale to support its decision and show the decision was made in good faith.

Consider, for example, e-mails sent by a parent of a special education student who has recently become increasingly upset with the school district. Imagine that this parent files for a due process hearing with the State Educational Agency. Although a due process hearing is not immediately subject to the Federal Rules of Civil Procedure, if the parent, or even the school district, chooses to appeal the administrative hearing committee's decision to federal court, the litigation would then be subject to the Federal Rules. Therefore, if a district has purged those relevant e-mail communications between the parent and school district from its system, even inadvertently, and they are requested in the discovery phase, the district likely will be subject to sanctions.

In the example above, the school district should have educated its special education staff to save both parent and school e-mails into a separate folder within the e-mail system. The teacher also should have printed out these e-mails and included the paper copies in the student's special education file. This portion of the records management policy should also be explicitly laid out in the school district's policy.

### ***Enforcing the Records Management Policy and Plan***

Once the school board records management policy and plan are in place, like any other job requirement, those staff members that utilize computers and other forms of communication technology as a part of their position should be evaluated as to their effectiveness at utilizing and managing ESI documents. As part of the evaluation process, evaluators should ask those staff members to show how they have implemented the records management system to ensure that they are properly managing ESI records in compliance with the records management policy and plan. If staff members are inadequately managing ESI documents, they must be held

accountable just as if they were failing at any other part of their job. They should be put on an improvement plan and evaluated periodically to ensure compliance. Failure to do so puts a school district at risk of potential liability in the face of impending litigation.

### **Caution – Safe Harbor Provision in the Law Has a Rocky Bottom**

Many school district officials have misinterpreted various attorneys' explanations of the "safe harbor" provision in the Federal Rules of Civil Procedure. It is true that the Federal Rules do state that "[a]bsent 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). However, the comments to the Rule clearly point out if an entity deletes items per its policy for the last three months, it should be sure to do the exact same thing during the current month. Thus, a policy should be consistent with the practice and enforcement of the plan, and the enforcement of the plan must be consistent from month-to-month.

Further, the "safe harbor" provision does not absolve a school district from deleting e-mails that the school district ***knew or should have known were relevant to a claim or a defense to a claim***. In this situation, the safe harbor provision does not help a district. Therefore, best practice dictates that school districts should educate each and every staff member who utilizes computers, laptops, voicemail, PDAs, and other electronic devices of what they are supposed to save and what they are allowed to delete according to the policy.

### **Conclusion**

The Federal Rules seem to have placed an onerous burden on school districts, but after consultation with the proper technology professionals and involvement of a school attorney, the implementation of an updated school board policy and an ESI management system will actually save the school district time, money, and resources in instances of impending litigation. Technology continues to increase in its complexity, therefore, many school districts have hired either a technology consultant or a full-time Management Information Systems (MIS) trained technician to manage the electronic records management policy and plan.

### **Sample E-mail Records and Electronically Stored Information Policy**

Any e-mails that are pertinent and must be saved for an extended period of time (to exceed one month) shall either be (1) printed and physically filed in such a way that they will be easily retrievable or (2) saved directly to an electronic file on one of the district computers from which it will be easily retrievable. The district should regularly delete unnecessary e-mails on the district's computer system on the first school day of each month during the school year.

Until the district's e-mail system can be equipped with such capabilities, all employees of the school district shall regularly update their e-mail account by either saving necessary and pertinent e-mails to their computer or printing them and filing them appropriately. Employees shall also delete unnecessary e-mails from their account at the same time. This process shall become a permanent and regular occurrence if the automatic deletion process is not incorporated into the district's e-mail system.

## **I** mplementing a Litigation Hold Applicable to Electronic Information

*By: Jill Robb Ackerman, Baird Holm, L.L.P, Omaha, Nebraska*

### **A Classic Scenario for an e-Discovery Disaster**

#### ***The Scene***

A lawsuit is filed on March 20 against a client school district concerning an employment incident that occurred the prior September. The lawyer calls and informs the superintendent that the school district needs to “locate relevant documents” and “not to destroy relevant documents.” The lawyer follows up the call with a “litigation hold” letter to the superintendent.

Upon receipt of the letter, the superintendent sends an e-mail to the principal and three teachers that likely have relevant information. The teachers set aside some files. A couple of the teachers print out a few e-mails and documents from their computers that they think might be relevant.

#### ***Six Months Pass***

On August 20, the opposing counsel sends out a Request for Production of Documents to the school district asking for relevant “electronically stored information” (ESI). The lawyer forwards the Request to the superintendent who circulates it to the principal and the same three teachers that received copies of the litigation hold letter. The lawyer then visits with the superintendent, and they determine that three more teachers were involved in the situation giving rise to the litigation that did not receive copies of the litigation hold e-mail. The superintendent’s assistant starts to gather the requested documents. The assistant calls the information technology (IT) department for the ESI, and the document nightmare begins to unfold.

### ***Flashback: What Happened to the “Documents” from September to August?***

Four weeks after the incident happened in September, the school district shifted to a new e-mail system. Before that, the school district was using an outside service provider to provide e-mail service. On the new system, backup tapes at the central office were overwritten nightly in the regular course of business. The central office e-mail server was set to automatically purge (*destroy*) all e-mails older than 90 days.

The principal’s computer crashed in April, and her hard drive was replaced. One of the three teachers initially notified of the hold resigned at the end of the year and his computer hard drive was wiped clean and reassigned to a new teacher. The remaining five teacher’s computers were acquired by a grant and were not managed centrally. Sometimes some of the data was backed up on zip drives at the school level. Three of those teachers had their computers set to purge e-mails from their machine on the last day of every school year, including the deleted files. One of the teachers diligently saved important e-mails to topical folders on her desktop.

#### ***The Consequences***

Not surprisingly, full compliance with the pending request for production in this scenario is impossible. Data was lost when the district shifted from an outside service provider to a new e-mail system and no attempt was made to transfer or preserve the data. Data also was lost when the central office server continued to auto delete information as the litigation progressed toward discovery. The crash of the principal’s computer lost more data that had been saved on

her personal hard drive. Data was lost when the district wiped clean the hard drive of the teacher who left. More data was lost when three of the teacher's e-mail accounts were set to purge on the last day of the school year. Finally, data was lost when the three teachers who did not receive notice of the litigation hold continued to delete information daily.

When relevant information, or information that can lead to the discovery of relevant information, is lost, courts can impose sanctions including default, dismissal, adverse inference, evidence preclusion, and costs for special masters and computer forensics experts. These sanctions can be imposed on clients, attorneys, and responsible individuals.

### School Law Practice Pointers

#### Key Steps to Effectively Implement a Litigation Hold:

1. Implement a records management plan before disputes arise.
2. Create an ESI team NOW!
3. Create a data map.
4. Identify preferred electronic discovery vendors before disputes arise to have the technical resources at hand to deal with unique situations.
5. Create the procedure for a litigation hold directive that can be modified to fit various situations.
6. Obtain the support of administration because litigation holds take time and resources to be effective.
7. Identify a responsible party at the school district and at legal counsel's office to monitor and enforce any litigation hold.
8. Before disputes arise, educate personnel about what a litigation hold is and what can happen if it is not taken seriously.
9. Follow up an initial litigation hold with face-to-face interviews with appropriate personnel to make sure all relevant data is being preserved.
10. Document and monitor the procedures followed.

### Avoiding the Disaster

Planning for a litigation hold as part of a records management plan in advance of litigation will reduce costs, provide strategic advantages in litigation, and minimize the chance for sanctions. A summary of the steps required to effectively plan for and implement a litigation hold are contained in the School Law Practice Pointers section below.

Courts have long recognized the duty to preserve relevant information. Courts expect entities to effectively implement a litigation hold. The adoption of the new Federal e-Discovery Rules is the catalyst that has heightened both the courts' and litigants' awareness of the necessity of an effective litigation hold procedure that stops the destruction of paper documents as well as the more voluminous and illusive ESI.<sup>1</sup> State courts are likely to place similar expectations on parties.<sup>2</sup>

#### What Is a "Litigation Hold"?

A "litigation hold" is simply a directive to parties not to destroy any documents, including electronically stored information in all of its various forms, that might be relevant to a legal proceeding, or that might lead to the discovery of relevant information.<sup>3</sup>

#### When Does the Duty to Implement a Hold Directive Arise?

The duty to preserve arises when there becomes a likelihood that potential litigation will occur. This duty often arises long before formal proceedings are filed.<sup>4</sup>

#### Who Is Responsible to Decide When to Implement the Litigation Hold?

The client school district is ultimately responsible for the litigation hold generally upon the advice of counsel. This is a matter that should be discussed with counsel long in advance of a dispute arising.

## **Create an Electronic Stored Information Team**

Preliminary work is necessary for an effective litigation hold. The best practice is to form an Electronic Stored Information Team (ESI team) as soon as possible. This team should include legal counsel, a designated school administrator, and personnel from IT.

This team should have a designated leader at the client level and a designated contact with legal counsel's office. These two people have the responsibility to ensure that the litigation hold is successful at both the client and the counsel's end. Due to the significant time commitment, the team must have the school administration's support.

## **What Are the Responsibilities of the ESI Team?**

This team will be responsible for understanding the language and status of current and former IT systems. Also, it will be responsible for creating, documenting, and enforcing the best practices procedure. It will ensure that "good faith" steps to preserve evidence are taken and documented to defend against possible allegations of spoliation. Most likely a member of the team will be the FEDERAL RULES OF CIVIL PROCEDURE 30(b)(6) witness that will be designated to testify as to the steps that were taken to preserve information or as to the type and location of ESI within the organization. This team also will be in place to assist outside counsel with the representations that will be made to opposing counsel and the court concerning ESI. This should minimize the risk of exposure to sanctions and court costs through proper management and improved accuracy.

The ESI team will understand the ESI format and locations before litigation arises. The team should identify the most common types of litigation facing the district and create an ESI discovery plan that can be applied in various types of litigation. The ESI team will need to be familiar with the records management plan. The team will be responsible for creating procedures for the litigation hold and the suspension of

document destruction that may be occurring under the records management plan or automatically due to settings on hardware that are interacting with the ESI.

## **Become Familiar with e-Discovery Vendors Before a Major Dispute Arises**

Currently, many e-discovery vendors are trying to capture market share in this extremely lucrative business.<sup>5</sup> Educate yourself about what services they offer and how they are priced before the need arises. Before purchasing a product, meet with several. Most are willing to meet face-to-face and demonstrate their products. A few good questions to ask vendors are: Do they have consultants to assist in data capture. How are those services priced? Does the vendor process the data into a format allowing the data to be reviewed for production? What type of review tools does the vendor support?

Meeting with the e-discovery vendors in advance helps counsel make informed decisions as to whether to perform certain tasks in-house or whether to out-source the work. Also meeting with the vendors helps educate counsel on the entire e-discovery process. It is necessary to understand the entire process to make reasoned decisions during the document hold and data capture process. After meeting with several vendors, select one or two preferred vendors that you can call on to assist at the various stages of the process.

## **Overview of a Hold Directive**

The actual implementation of the hold directive within a school district necessitates the cooperation of counsel, the administration, fact witnesses, and IT. The relevant current and ongoing data will need to be preserved and at least portions of it gathered. The ESI team will need to determine the nature and extent of the affected departments and the records custodians within the departments. Explicit written notice must be given to the affected parties letting them know what to hold and how to hold the data. Procedures must be in place to address employee turnover to ensure that data is not lost when computers are

reassigned. Automatic deletion and over-writing of backup tapes will have to be modified to preserve relevant data. Personnel must be trained and compliance must be monitored.

### Create a Data Map

Before an effective litigation hold can be in place, the ESI team must know what types of ESI exist and where the ESI is stored by the various custodians. Therefore, creating a “data map” that tracks the custodian’s ESI to the various locations where it is stored is an important early step. This should result in added assurance that the appropriate information is preserved.

A data map identifies the types of ESI that may be affected for example: e-mail and attachments,<sup>6</sup> voice mail, databases, spreadsheets, word processing documents, newsgroups, backup files, directories, internet histories, security and access information, cache files, other lawsuits, faxes, and metadata. The data map will identify the possible storage locations of the ESI such as service providers, computers, laptops, servers, backup computer files, archives, legacy data, firewalls, audit trails and logs, PDAs, cell phones, pagers, printers, scanners, and digital cameras. The data map also will identify the possible storage media which may include hard drives, floppy disks, CDs, DVDs, zip disks, smart cards, micro-film, and memory stick drives also known as “flash,” “jump,” “keychain,” or “thumb” drives.

Without a data map, it is difficult to impose a hold directive that will be effective. It is too easy to overlook either the type of data or the location of storage.

### Litigation Hold Directive Procedure

The school district with the assistance of counsel must determine which data sources have potentially relevant data.

The hold directive procedure should begin with an analysis of the factual issues relating to the legal matter and a discussion with counsel, the client, and IT to determine who may have data

relevant to the dispute and where it is stored. Analysis must be made to determine whether to hold only relevant information or to hold everything. This decision will likely turn on the complexity of the case.

Next, identify the departments that may have relevant data. Then identify all custodians that may have relevant information.

Finally, send out a specific litigation hold directive to all affected personnel clearly labeled ATTORNEY/CLIENT AND WORK/PRODUCT PRIVILEGED. This memo should explicitly direct the custodian not to delete anything from any computer he or she is using, or destroy any hard copies of school related documents until further directions.

In a recent case, *Gibson v. Ford Motor Co.*, No. 1:06-cv-1237-WSD, 2007 WL 41954 (N.D. Ga. Jan. 4, 2007), the court held that the litigation hold directive was protected by the attorney client and work product privileges and was not discoverable. The court found that the directive was created by counsel, drafted after the dispute arose, related solely to lawsuit, and existed for purposes of the defendant responding to discovery requests.

### What Does a Litigation Hold Look Like?

Page 10 of this article contains two samples of litigation hold directives that can be modified to fit narrower or broader disputes.

### Inform IT of the Litigation Hold

The IT department (or any other entity)<sup>7</sup> responsible for the information system should implement the litigation hold by:

1. Suspending the normal document retention/destruction policy.
2. Informing and continuing to remind all personnel to cease deleting any documents related to the legal issue. Issuing the notices contained on page 10 is the first step in this regard. Thereafter periodic reminders must be sent.

3. Changing any switches in the e-mail system, including on individual computers, that would automatically delete or alter data.
4. Stopping the automatic recycle of backup tapes.
5. Stopping the automatic recycle of personal computers. This is important if the school has a practice of reassigning a computer from a departing individual to a new individual within the school. Oftentimes in this reassignment process, the hard drive of the computer is erased. Prior to such erasing, it will be necessary to identify and preserve any school-related documents on the hard drive.
6. Make an image clone of the hard drives of any computers assigned to individuals who may be key to the litigation.

### **Follow Up the Litigation Hold Memo with Face-to-Face Meetings with Custodians**

Document the list of affected departments and custodians. Counsel and the designated member from the ESI team then should interview each custodian that may have relevant information. Document these meetings. The interviews should cover where the custodian stores ESI information that relates to the dispute. Start with identifying the servers, and then check local drives, laptops, home computers, thumb drives, CD's, and DVD's. Do not forget to also discuss where hard copies of relevant documents are stored. Document the nature and storage location of this information.

### **Maintain the Integrity of the Data**

Arrangements should be made to copy the ESI identified in the face-to-face meetings using a method that does not alter metadata that may become relevant in the dispute.

The best method to maintain the integrity of the data is to make a "forensic copy" that reflects both the allocated and unallocated space on a storage device.<sup>8</sup> When a forensic copy is made, a "write blocker" tool will be used to prevent the disk from being modified during the acquisition and examination.

Making a forensic copy is not always practical. The next best procedure is to make a "backup copy" with a program that will capture the data without changing the metadata.<sup>9</sup> That method captures the data but not the unallocated space on a disk. Be sure to make duplicate copies of the data and store the copies in different locations.

### **Follow Up the Litigation Hold with a Detailed Plan with IT Addressing Backup Tapes**

You will have to work with IT to determine how to handle the problem of backup tape data. Suspending the reuse of backup tapes can be extremely expensive. Obtaining technical assistance from an electronic discovery vendor is recommended at this stage.

Backup may be completed each night with monthly and annual backups. Backups may be made incrementally by backing up only new data. It is important to not destroy relevant information by overwriting backup tapes. Reusing a backup tape may well destroy information that is relevant to the lawsuit. There simply is no easy or inexpensive answer to the issue of backup tapes. Under the new FEDERAL RULES OF CIVIL PROCEDURE while a client may not have to produce what is on disaster backup tapes, the client is still obligated not to destroy what is on the tapes.

Going forward in the lawsuit, it may be possible to shift the relevant custodian's ESI to a separate server and suspend reuse of backup tapes on that server.

### **Monitor the Legal Hold**

It is critical to designate someone at the client level, preferably the member of the ESI team, as well as someone at the counsel's office, to monitor compliance with the litigation hold. Documentation of the identification, preservation, and capture of the data must be maintained. Periodic reminders must be sent and should be followed with routine direct contact with the custodians. These reminders should be documented. The person responsible for monitoring the implemen-

tation of the litigation hold must track the custodian's storage devices and note any changes. If an employee leaves, steps must be taken to preserve the ESI on his or her computer. If computers are changed, again, steps must be taken to preserve the existing data. Finally, if system conversions occur, the person monitoring must be sure the conversion is documented, as well as the steps taken to preserve all affected ESI.

### What About the Safe Harbor?

FEDERAL RULE OF CIVIL PROCEDURE 37 provides that "absent exceptional circumstances, a court may not impose sanctions...on a party for failing to provide electronically stored information lost as a result of a routine, good-faith operation of an electronic information system."<sup>10</sup>

A well-developed ESI plan properly followed, enforced, and documented will increase the chances that the "safe harbor" will provide protection from sanctions. Good faith will be determined on a case-by-case basis. Good faith will require reasonable efforts to suspend or modify features of routine operation, such as "auto-delete," to prevent the loss of information. Relying on the safe harbor should be the exception, not the norm.

### Conclusion

The scenario described in this article is a realistic illustration of what could happen if a school district fails to consider the preservation of electronic evidence before litigation occurs and fails to properly implement a litigation hold in the event of litigation. Given the volume of electronic information, it is probably unrealistic to think that even the best litigation hold policy and practice will identify and preserve every piece of relevant electronic information. Nevertheless, a well-planned and well-executed litigation hold probably could have eliminated all of the major data holes that will exist in the above scenario. Preparing to implement such a hold is time-consuming and may require conquering a steep learning curve. However, the rewards are great: the client school district will have the evidence it needs to defend itself during litigation without the threat of court sanctions and other negative consequences.

### Sample Notice Regarding Preservation of Historical Documents

If you saved e-mail from any prior e-mail system which may contain school-related documents, do not delete or destroy any such e-mail or the related system files (for Microsoft Outlook those files have a ".pst" extension). A **school-related document** is any e-mail, word processing document, spreadsheet, text document, or other document (whether in *electronic* or *hardcopy* form) related to school business or school matters.

If you saved any school-related documents to:

- your local workstation,
- the "home directory" of your school's network,
- a home computer, or
- any portable device (including laptops),
- any flash or thumb or similar portable drive,

then do not delete or destroy any such school-related documents.

If you have made your own personal backup copies of any school-related documents on tape, diskette, zip drives, CD-ROM, or any other media, please maintain those backups. Do not recycle, destroy, or reuse such backups.

Do not destroy or purge any hard copies of school-related documents. However, this does not include advertisements or duplicate paper documents that do not have handwriting or other notes on them.

If you have any questions please contact:

### Sample Notice Regarding Preservation of Current Documents

On an on-going basis and until further notice, do not delete or destroy any school-related documents. **School-related documents** include any e-mails, word processing documents, spreadsheets, text documents, or other documents (whether in *electronic* or *hardcopy* form) related to school business or school matters.

## Endnotes

1. On December 1, 2006, the U. S. Supreme Court e-Discovery Rules became effective. The specific term “electronically stored information” was added to FED. R. CIV. P. 16, 26(a), 33, 34, and 45 to explicitly include all the various forms of electronic information which are rightfully subject to discovery. The changes to the rules now require an attorney to understand: (1) the nature and existence of ESI early in the litigation; (2) the form ESI is maintained; (3) how to preserve ESI; (4) how privileges will be handled; and (5) how to implement procedures to establish good faith compliance with the rules.
2. During November of 2006 the National Uniform Conference of Commissioners on Uniform State Laws proposed a draft of laws for states based on the Federal Rules.
3. FED. R. CIV. P. 34(a) provides that “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.”
4. MICHAEL R. ARKFELD, *ELECTRONIC DISCOVERY AND EVIDENCE*, § 7.9 at 7-129-33 (Law Partner Publishing 2006-7). Variations exist among the jurisdictions as to when the duty to preserve evidence arises. Counsel for the district should be familiar with the specific case law from the relevant jurisdiction.
5. For example, Krroll Ontrack,<sup>®</sup> [www.krrollontrack.com](http://www.krrollontrack.com); Lexis Nexis Applied Discovery,<sup>®</sup> [www.lexisnexis.com/applied-discovery](http://www.lexisnexis.com/applied-discovery); Merrill Corporation, [www.merrillnavigator.com](http://www.merrillnavigator.com); Focus Legal Solutions,<sup>®</sup> [focussolutions.com](http://focussolutions.com); just to name a few, are experienced e-discovery vendors. Each offers somewhat different solutions to problems. Often local vendors offer e-discovery services that may provide satisfactory solutions and assistance for smaller cases.
6. Preservation, capture, processing, and review of e-mails and attachments is the most expensive aspect of e-discovery. Costs can be reduced somewhat if mainstream e-mail systems are used such as Microsoft Outlook<sup>®</sup> or IBM Lotus Notes<sup>®</sup>. Many of the electronic tools that have been developed to assist in e-discovery make the capture and review of relevant e-mails in these applications easier, though still expensive. In contrast, from an e-discovery perspective, it is very difficult to capture, due to the structure of the application, a subset of relevant e-mails and attachments in Open Text’s First Class<sup>®</sup> e-mail system which is used in many school districts. Working with that system is much harder in the e-discovery context.
7. Many times schools rely on outside service providers to store data.
8. BRIAN CARRIER, *FILE SYSTEM FORENSIC ANALYSIS* (Addison-Wesley 2005). This is a high-level book that explains the complexity of forensic analysis of computers.
9. Programs such as Symantic’s “Ghost<sup>®</sup>” are sometimes used to capture data. Be sure to understand the limitations of such programs and the impact they may have on the integrity of the data before authorizing data capture using such a program.
10. FED. R. CIV. P. 37(f).

### School Law Practice



Lisa E. Soronen, Editor  
& Senior Staff Attorney  
Andrew Paulson, Designer  
& NSBA Web Coordinator

*School Law Practice* is an electronic publication of the NSBA Council of School Attorneys and can be purchased for \$20 per issue on the Council’s E-docs Store at <http://www.nsba.org/cosa>.  
ISSN: 978-0-88364-298-6.

Copyright © 2007 by the National School Boards Association. All Rights Reserved.