

INFORMATION PAPER
FEBRUARY 2011

Email Archiving:

What Schools Need to Know — and Do



Lightspeed
Systems

Network solutions for safe online learning

Introduction.....	3
eDiscovery Regulations.....	3
Backup vs. Archive.....	4
Why Archive?.....	4
State-Specific Regulations	6
What It Means for Schools	7
Best Practices for Email Archiving	7
Creating a Data Retention Policy.....	8
Implementing an Email Archiving Solution.....	8
Lightspeed Email Manager	9
A Comprehensive Solution	12
Testimonials.....	13
Conclusion	14
About Lightspeed Systems	14

Introduction

No matter the organization type, today's business communication relies heavily on email and instant messaging. In 2007, IDC predicted that nearly 97 billion emails, with 40+ billion attributed to spam messages, would be sent daily worldwide.¹

Simply handling that level of traffic has been difficult for many school districts, in which resources are scarce and the latest technology may be out of reach.

Adding to the difficulty: the need to retain that email data for easy retrieval.

Today, data retention is necessary for several reasons: to comply with federal eDiscovery regulations and state retention schedules, to respond to lawsuits, and to manage organizational knowledge. To effectively and efficiently meet those needs, districts require a solution for email archiving that encompasses all inbound, outbound, and internal email and instant messages ensures storage, search, and retrieval—and that minimize both costs and staff time.

eDiscovery Regulations

In 2006 the Federal Rules of Civil Procedure were amended by the Supreme Court to cover the “discovery of information” in civil cases, including electronic information such as emails. Failure to comply with these regulations, preserve and produce electronically stored information (ESI) in a timely fashion could open districts to fines and other penalties.

In its paper on the subject, the Consortium of School Networking (CoSN) summarizes the eDiscovery law:

“These are the legal rules that dictate what happens in federal civil cases and how discovery of information and materials relevant to civil cases is conducted. Under the rule change, all electronic information is subject to legal discovery. Failure to produce such documents may lead to sanctions, including monetary fines and adverse court rulings in the underlying case.”³

Among the changes in the FRCP amendments,

- ESI is broadly defined and clearly subject to discovery
- Parties to litigation are required to meet and plan for electronic discovery
- A distinction is recognized between ESI that is readily versus not readily accessible, the latter of which may only be required to be disclosed pursuant to “good cause.”
- Procedures established for asserting claims of privilege (Ex. Attorney-client) to ESI
- Protection from sanctions (“safe harbor”) for parties who destroy or delete ESI pursuant to a good faith and routine operation of a District’s information systems.

¹ http://findarticles.com/p/articles/mi_m0EIN/is_2007_April_9/ai_n18791999/

For example, upon "showing of good cause" for disclosure, most emails among the interview committee members for an administrative position which is now the subject of an EEOC, Title VII complaint of discrimination would need to be produced in their original form and include information such as file owner, creation date, routing details, sender, receiver and subject line. With these requirements, the need for a full email archiving solution is evident: searching traditional tape backups for requested data can be a time-consuming and costly endeavor. One California school district estimated the cost at \$20,000 after discovering it would need to re-build a replaced Exchange Server 2000 in order to retrieve and read the data stored on tape. And yet, the penalties for intentionally or even negligently destroying ESI have been far, far greater—in one infamous case resulting in a default judgment of \$1.58 billion dollars against Morgan Stanley. Having an email archiving solution in place can go a long way to protect school districts from incurring such costs.

Backup vs. Archive

The volume of email alone makes retention and storage a daunting task. Historically, storage demands have been met using backup tapes. However, backup tapes are not easily searched—creating expensive disruptions when a message needs to be retrieved. Attachments, increased volume, and growing message sizes create more difficulties for efficient search and retrieval.

To meet today's legal and practical requirements, as well as to handle the growing amount of email communication that needs to be retained, backups are not a viable or acceptable option.

The problems with backups:

- Backups do not save *all* data.
- Backups are alterable, and lack of data integrity can open the process to scrutiny.
- Backups are difficult or impossible to search.

Backups serve a purpose. But their purpose is not email archiving:

Backup: preserves data against failure or disaster, not for accessing data in its raw state

Archive: securely preserves data for easy access in a non-production environment

Why Archive?

Email archiving allows school districts to meet eDiscovery regulations, as well as reap additional benefits. But for many districts, the challenges have made implementing a full email archiving solution a daunting task.

Challenges of archiving

Many districts have not implemented an email archiving solution because of:

- Lack of clear direction about regulations
- Lack of money to purchase new software/hardware
- Lack of time and resources to manage an additional solution
- Lack of solutions built for their specific needs (rather than business needs)

Benefits of archiving

With an effective email archiving solution in place, schools will be able to:

- Respond to legal requests more efficiently
- Save costs and staff time
- Leverage archived email as a knowledge store
- Lower risk and exposure
- Implement disaster planning and recovery practices
- Meet eDiscovery regulations

Why schools need an email archiving solution

To comply with federal eDiscovery rules, and to protect themselves and prepare a framework for effective storage of electronic information, districts need to implement an email archiving solution now.

Lawsuits. Any court of law can request or subpoena data or information relevant to a lawsuit. Also, sometimes the right email can thwart a potential lawsuit. For example, in Title IX litigation against public school districts, it is crucial that the school be able to demonstrate that some corrective action was taken against a staff member or student who may have harassed another student.

Lightspeed Email Manager allows the District to quickly and confidently retrieve electronically communicated corrective measures. In any case, plucking some messages out of the email haystack can be easy or difficult, depending on how they are stored. The digital originals will be critical since once an email is sent, the sender has virtually no control over what happens to it. Without knowledge or consent, that email can be printed, forwarded to others, edited, and changed dramatically. The potential to alter the content of emails (and the importance of identifying digital originals) can be especially concerning when, for instance, an employee of the district received legal advice from the school district's lawyer or legal team in electronic form and now seeks to defend or obfuscate their own conduct by "editing" the guidance they received.

Organizations can protect themselves against unwarranted claims by establishing policies and procedures that capture inbound, outbound, and internal email messages as business records. Regrettably, without email archiving in place, the cost of producing the needed information can outweigh the damages claimed.

Knowledge management. Email has become a part of the organizational knowledge base by virtue of the vast amount of intelligence that is not replicated in any other data. Michael Osterman, president of

messaging and collaboration research firm Osterman Research, believes "companies will see the value of email as a source of knowledge increasing, primarily because this will be one of the key secondary benefits that organizations derive after they have deployed an archiving solution."²

State-Specific Regulations

Many states have also created or updated their own specific guidelines for eDiscovery and/or electronic data retention, augmenting or supplementing the federal rules. Currently, 23 states have their own guidelines related data retention and ESI. A table outlining those state-by-state guidelines has been compiled by **K&L Gates LLP**.³ As you create and implement your district Data Retention Policy, be sure to check with your district legal team and consult your state legislature for the latest information.

Data retention also rules vary by state. You can begin research into your state's specific guidelines here:

<http://www.ediscoverylaw.com/2008/10/articles/resources/current-listing-of-states-that-have-enacted-ediscovery-rules/>

But be sure to consult with your district legal team when establishing policies.

The latest update to the eDiscovery landscape, a newly passed bill in California, is expected to provide a baseline that many states will follow.

California Assembly Bill 5, otherwise known as Chapter 5 - Electronic Discovery Act, was signed into law on June 29th, 2009.⁴

Some key points of the California Electronic Discovery Act:

1. It requires data to be produced in "a reasonably useable form."
2. It requires testing and sampling of ESI.
3. It opens the door to monetary sanctions for failure to meet eDiscovery regulations.
4. It allows for a "good faith" exemption to those monetary sanctions.

² <http://www.intradyn.com/docs/emailmining.pdf>

³ <http://www.ediscoverylaw.com/2008/10/articles/resources/current-listing-of-states-that-have-enacted-ediscovery-rules/>

⁴ <http://estorian.dcginc.com/2009/09/california-new-ediscovery-law.html>

What It Means for Schools

Many districts have been taking a wait-and-see approach: waiting for a case in which a school district violates these regulations; waiting to see what the repercussions are; waiting for more specific guidance; waiting for funding....

But school districts can't afford to wait any longer.

According to Keith Krueger, CEO of the Consortium of School Networking (CoSN):

“E-mail has transformed the way we all communicate—educators, schools and school districts included. Because much information is shared electronically and federal laws and judicial interpretations are including electronic communication as subject to legal discovery, it has become increasingly important for schools to make e-mail archiving a critical part of their record-keeping activities.”⁵

School districts must protect themselves against costly litigation, regulatory non-compliance, fines, and penalties by implementing an email archiving solution now.

Best Practices for Email Archiving

Creating a policy for email archiving, selecting a solution, educating users, implementing policies, and monitoring the solution may seem overwhelming to under-staffed school IT departments. But as a starting point for your email archiving endeavor, consider these best practice recommendations:

- Create a Data Retention Policy.
- Bring together representatives from IT, legal, and human resources departments to formulate a sound and viable email archiving plan.
- Instruct users not to consider anything written or received on a school-provided email account to be private.
- Archive emails in accordance with the statute of limitations on civil litigation in your state and/or the recommendation of your legal department.
- Check your state guidelines. Many states have provided additional requirements—as well as specific guidance—for eDiscovery in their state.
- Monitor any solution you implement on a regular basis to ensure that it is working and document your ongoing efforts to maintain an effective solution.
- Be sure to secure your email archive to prevent unwanted access to personal information.

⁵ <http://thejournal.com/Articles/2008/06/27/CoSN-Details-Changes-to-EMail-Regulations-Calls-for-Comprehensive-Solution.aspx>

- Create a “litigation hold” strategy. This is a requirement if you are ever named to a lawsuit. As a best practice, you may also use this strategy proactively: for example, copying an employee’s hard drive and specifically archiving emails in the event of an employee termination for misconduct of any nature, or when an employee has logged a complaint against other school officials or the District.

The essential things schools must do now:

1. Create a Data Retention Policy.
2. Implement an email archiving solution.

Creating a Data Retention Policy

One of the key elements to eDiscovery compliance is creating and following a reasonable data retention policy. The specifics of your policy will vary, depending on state requirements and district decisions. However, your policy should clearly detail:

- The procedures that will be used for email archiving
- The solution(s) that will be used for email archiving
- How long emails and other data will be stored
- Training procedures for staff
- Procedures for monitoring the system

In fact, having a comprehensive policy in place *as well as* a solution for email archiving may protect a district even in the event that they are unable to produce ESI upon request. For example, the federal eDiscovery rules may shield a district from penalties for destroying ESI if the data was deleted in “good faith” while following established data retention procedures. To this extent, it is often helpful that the district actually has and consistently follows a data retention schedule.

Implementing an Email Archiving Solution

The challenges of email archiving, as listed previously in this information paper, included lack of information and direction about the regulations. The first section of this information paper aimed to clear up confusion and provide a clear direction for schools. The other challenges were: lack of money to purchase a solution, lack of resources to implement a solution, and a lack of solutions built for the education market.

Lightspeed Email Manager is a powerful solution that can help schools address those challenges. It offers a cost-effective and easily-managed solution designed specifically for schools.

Lightspeed Email Manager

Lightspeed Email Manager helps you easily conform to federal and state eDiscovery regulations with comprehensive email archiving.

Lightspeed Email Manager provides key features for eDiscovery compliance:

- **Comprehensive capturing and indexing** of message attachments as well as full message details
- **Time-stamped and unalterable file integrity** for the archived data
- **Archival of inbound and/or outbound SMTP** traffic and attachments (including documents, programs, and multimedia files)
- **Message file storage** with indexing parameters for: From, To, Subject, Date, Keywords, and Body Text
- **Flexible configuration** of data redundancy rules of archived email (backup servers)
- Optional journaling of internal email processed by mail-server journaling agents
- Optional "keyword" monitoring, indexing and reporting
- Using Microsoft SQL, dual indexes are maintained for 'Current Messages' and 'Archive Messages' to provide faster search processing when performing network traffic analysis or historical message analysis and retrieval.
- Full retrieval and flexible 'Forwarding' of archived messages and attachments
- Single-instance archiving of message attachments (no duplicated attachment files)
- Indexing and archive capacity limited only by available disk storage

Easy Compliance with Lightspeed Email Manager

Compliance rests on three prongs: unaltered email retention, security, and auditability. Lightspeed Email Manager meets them all.

"Digital Original" Retention. Through inline security servers and hooks in the email servers, original emails and attachments are indexed and stored for the number of years determined necessary by organizational policy.

Security. Database access is limited to designated individuals with proper credentials for searching and retrieving messages.

Auditability. Messages from all email servers on the network may be searched through a central, web-accessible interface.

Easy Implementation with Lightspeed Email Manager

For schools to implement an email archiving solution, it must offer functionality, ease of use, and affordability. Lightspeed Email Manager offers key features and benefits in each category.

Powerful Functionality

- Imports all email into the archive upon setup
- May be searched even when email service is down
- Rapidly retrieves recent email kept in a separate index (e.g., last 60 days)
- Offers daily updates, scans for and eliminates viruses

Ease of use

- Enable basic end-user searches on sender, recipient, subject, and date range
- Extended administrator searches on keywords, attachments, meta info, body text, and "suspicious phrases"
- "Retrieve Mail" link on every report allows quick, easy forwarding
- Tightly integrates with Microsoft Exchange Server 2003, Novell GroupWise, POP3

Affordability

- Lightspeed Email Manager, with its powerful email archiving capabilities, is included at no extra cost with Lightspeed Total Traffic Control, our all-in-one solution that includes Internet filtering, spam blocking, anti-virus, bandwidth management, and detailed reporting
- Or, with a small per-mailbox fee, you can purchase Lightspeed Email Manager as a standalone component
- Archived files are compressed to save space on your server and minimize hardware requirements
- To save space, if the same attachment is sent to multiple recipients, it is intuitively saved only once

Lightspeed Email Manager is a comprehensive email archiving solution built specifically for schools.

How Lightspeed Email Archiving Works

1. Email and/or Instant Message items are processed by IpmArchive.exe. As per the Message Journaling Properties options: Incoming and Outgoing mail messages are processed via SMB retention; Internal mail messages, which can include POP3, are placed into the TTC Server's Message Journaling Queue (C:\Program Files\Lightspeed Systems\Traffic\Mail Archive\Queue), and Instant messages are created from database report records.

Inbound and Outbound Email Traffic

Inbound and outbound SMTP messages are retained into **Mail Archive/[yyyymmdd]** folders by the Spam Mail Blocker Object. Every five minutes IpmArchive.exe process indexes and archives all newly retained ham (clean) and outbound Spam Mail Blocker messages.

Internal Email Traffic

Email messages are added directly into the Message Journaling Queue by one of the Message Journaling Agents. The next IpmArchive.exe run will index and archive the new messages.

POP3 Connector

Every five minutes the Pop3Connector.exe process connects to the defined POP3 Journaling mailbox to copy new messages to the TTC server Message Journaling Queue. The next IpmArchive.exe run will index and archive the new messages.

Instant Messages

The IpmArchive.exe process retrieves new IM traffic records from the Statistics database (the content from the **Instant Messaging** report), then indexes and archives as messages. The IM From, To, Subject and Message are archived.

2. The items in the Message Journaling Queue are processed, indexed, and journaled (archived). The journaling process (IpmArchive.exe):
 - a. Copies every file into a subfolder for each backup journaling server that has been configured in the local Message Journaling properties.
 - b. Scans each file for custom keywords and suspicious phrases (specified in Message Journaling properties) and creates search index entries for these items.
 - c. Indexes message data, such as:
 - From Address/ID
 - To Address/ID
 - Subject
 - Date
 - Body text
 - Attachments
(Attachment files receive unique File ID's and are NOT duplicated in the journaling process, regardless of the number of email recipients or senders that an individual attachment is related to.)
 - d. Builds a cryptologic File ID (SHA-1 hash), based on the full content of the message file.
 - e. Generates a unique file name based on the first 10 kb of the message file.
 - f. Archives the message to the specified storage location
 - g. Creates an index file record for its 'File ID', 'File Name' and a sequential 'Document ID'.
 - h. Deletes the journaled file from the 'Queue' folder.
 - i. The Message Journaling task also looks for a Backup subfolder in the Message Journaling Queue. The existence of the Backup subfolder signifies that the local TTC server has been configured as a backup journaling server by another TTC server. If the Backup folder exists and there are files within the folder, the Message Journaling process will be performed for each of the files contained within.

3. When the local TTC server's Message Journaling properties have configuration entries for backup TTC Servers, the IpmIndex.exe program will periodically launch the 'backup' Message Journaling task (IpmArchiveBackup.exe) to make sure that backup copies of journaling files get passed to the configured backup servers.

The IpmArchiveBackup.exe program first locates any backup journaling folders inside the Message Journaling Queue folder. If any of the folders contain files, those files are copied into the '**Backup**' folder on the associated server.

For example, the contents of C:\Program Files\Lightspeed Systems\Traffic\Mail Archive\Queue\Oceania are sent to the **Oceania** TTC server and copied into the C:\Program Files\Lightspeed Systems\Traffic\Mail Archive\Queue\Backup folder. The contents of the Oceania server's Backup folder will be subsequently processed by the IpmArchive.exe program as outlined above.

A Comprehensive Solution

Lightspeed Email Manager can give your district far more than a solution for meeting email archiving requirements. In fact, the complete reliability with which ESI is preserved by the Email Manager, combined with the archiving and reporting options, allow your district to confidently integrate raw data with the ESI retention schedule you create per state law and your district's particular needs and resources.

Reporting

Reporting options for Lightspeed Email Manager email archiving include comprehensive searching for archived items by suspicious keywords and phrases, custom keywords, sender and receiver IDs, subject text, and message body text. The journaling function indexes all mail traffic in a SQL database and archives the mail and attachments for extensive reporting, flexible searching and long-term retrieval. Reports provide the ability to search and retrieve mail, as well as view the most active email users on your domain.

Complete Communications Management

In addition to comprehensive email archiving capabilities, Lightspeed Email Manager provides powerful spam blocking, email management, and email content filtering.

A Complete, Cost-Saving Network Solution

With school budget cutbacks on the rise, schools need to find ways to reduce expenses across the board—including within their IT departments. Lightspeed is committed to helping school IT staff manage and protect their networks while delivering essential educational services—while reducing expenses.

Lightspeed Email Manager is available as a standalone solution or as a component of Total Traffic Control, which brings together our component solutions into a single, comprehensive cost-effective, time-saving solution. Total Traffic Control gives schools the email archiving solution they need, while also providing other essential network functions at a low single cost-per-workstation.

Total Traffic Control includes:

Web Access Manager - Ensure safe web browsing with customizable filtering and features for safe Web 2.0 access.

Email Manager - Archive and report on communications, while blocking spam.

Security Manager - Block viruses, spyware, and malware with desktop and gateway security.

Network Traffic Manager - Control traffic with bandwidth management.

Power Manager - Manage energy use with automated power management. (optional add-on)

In addition, the solution is available as the Lightspeed Rocket, Email Manager, an appliance-based solution for high-capacity networks.

Lightspeed Total Traffic Control provides compliant email archiving, as well as other essential functions for a school network, in a single cost-saving solution.

Testimonials

"After setting the policy to archive email for two years, Lightspeed's Message Journaling puts the district on solid ground for any future inquiries."

-- Mark McMurray, Technology Coordinator, Frenchtown School District

"The regulations are vague, but some email archiving is necessary and Lightspeed makes archiving, searching and retrieving messages easy and usable. Lightspeed gives the process a nice and user-friendly interface."

-- James Hanrahan, Systems Support Specialist, Kenosha Unified School District

"We weren't doing email archiving at all before, and there was always a question of what the requirements were and what the cost would be. But by adding email archiving as a service on our network through Total Traffic Control, there was almost no extra cost."

--Tom Hafemann, information systems manager, Campbellsport School District

"Email Manager securely archives all emails without changing the data. This is important because if it changes the content in any way, it's not admissible in court."

-- Jim Gaydusek, Senior Technician and Server Administrator, Shelley School District 60

Conclusion

Federal eDiscovery regulations have been in place since 2006, but many schools have yet to implement an email archiving solution. At the same time, new state regulations and data retention schedules as well as the increasing risk of penalties make waiting a dangerous (and potentially costly) strategy.

Lightspeed Email Manager offers a comprehensive and compliant email archiving solution built specifically for schools, with additional features and benefits to help schools better manage their communications and networks while easily and cost-effectively meeting eDiscovery regulations.

About Lightspeed Systems

Lightspeed Systems Inc., founded in 2000, develops comprehensive network security and management solutions for the education market. We are committed to helping schools operate their networks effectively and efficiently, so educators can provide safe online teaching and learning environments.

Our software is used in more than 1,000 school districts in the United States, the United Kingdom, and Australia to protect more than 5 million students. For the past two years, Lightspeed Systems has been recognized on the Inc. 5,000 list as one of the fastest-growing private companies.

www.lightspeedsystems.com

- Watch a 5-minute overview of our solutions:
http://www.lightspeedsystems.com/resources/Lightspeed_TTC_Demo.html
- Register for a live web demo:
<http://www.lightspeedsystems.com/demo/>
- Get more information on this and other important topics in our Resource Center:
<http://www.lightspeedsystems.com/resources/Default.aspx>

Learn more about eDiscovery and email archiving:

Yale Law Journal – Overview:

<http://www.yalelawjournal.org/the-yale-law-journal-pocket-part/procedure/an-overview-of-the-e%11discovery-rules-amendments/>

COSN Report, *School Districts, Data Retention and Federal eDiscovery Rules: The Case for a Full Email Archiving Solution Now*, Executive Summary:

<http://www.cosn.org/Resources/ResourceLibrary/tabid/4189/id/26/Default.aspx>

Education Law Newsletter – The eDiscovery Question:

[http://www.stutzartiano.com/article_pdfs/E-Discovery%20formatted%20for%20Web%20\(use\)%20\(S7032972\).PDF](http://www.stutzartiano.com/article_pdfs/E-Discovery%20formatted%20for%20Web%20(use)%20(S7032972).PDF)

California Assembly Bill 5:

http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_0001-0050/ab_5_bill_20090629_chaptered.html

Information for other states:

<http://www.ediscoverylaw.com/2008/10/articles/resources/current-listing-of-states-that-have-enacted-ediscovery-rules/>

Electronic Discovery Reference Model:

<http://edrm.net/>

eDiscovery amendments summary:

<http://www.ediscoverylaw.com/2006/12/articles/news-updates/ediscovery-amendments-to-the-federal-rules-of-civil-procedure-go-into-effect-today/>