EduRisk™ By United Educators

HuronLegal

E-Discovery Toolkit for Educational Institutions

This toolkit, developed by Huron Legal, an e-discovery consulting firm, and United Educators, is designed to guide member institutions through the e-discovery process. The kit includes:

1. Guide to Preserving Data for E-Discovery

An institution must preserve relevant documents, emails, and records upon receiving notice of a lawsuit or events that are likely to trigger litigation. This guide provides a roadmap for:

- Deciding when document preservation is necessary
- Determining the scope of preservation
- Implementing preservation processes
- Defining ongoing responsibilities during litigation

The e-discovery process—the search of electronic records for use as legal evidence—can cost educational institutions thousands of dollars and hours. The proliferation of electronic communication means that your institution needs to be prepared when e-discovery becomes part of a lawsuit.

2. Sample Preservation Directive

This template for institutions needing to issue a preservation directive can be tailored to fit an institution's structure and the nature of the triggering event. In most situations, legal counsel for the institution should review preservation directives before they are issued.

3. Script and Checklist for Data Custodian Interviews

"Data custodians" are individuals who may possess records or documents that need to be preserved. This sample script and checklist provides guidance for information technology (IT) and legal professionals who interview data custodians to locate records within the scope of a preservation directive.

4. Sample Data Collection Tracking Charts

Institutions collecting data in response to an e-discovery preservation directive need a way to track the data as it is searched and culled by attorneys and e-discovery vendors. These tracking charts document the "chain of custody" and ensure data is not lost in the review process.

1. Guide to Preserving Data for e-Discovery

As soon as an institution receives notification of a lawsuit or at the time it reasonably anticipates potential involvement in a legal matter, the institution must decide whether it needs to preserve documents and data. This toolkit resource explains how to determine what to preserve and how to ensure compliance.

Deciding Whether to Preserve

The institution should designate a team of key personnel (commonly called the "eTeam") to make preservation decisions when an actual or potential legal matter arises. The first step is to determine the initial scope of the pending legal matter and decide whether there is an obligation to preserve potentially relevant evidence. The following is a list of potential triggers of a preservation obligation:

- **An actual or potential legal filing:** The filing of a complaint against the institution or any of its employees, the serving of a summons, or the filing of an administrative notice automatically triggers a preservation obligation.
- **Notice of a credible threat of a legal filing or litigation event:** "Credible threats" could include a letter from an attorney indicating that legal action is imminent, notice that an official administrative filing is forthcoming, or any other communication that formally discusses the possibility of a specific legal filing or litigation event.
- **Internal institutional events:** These events include but are not limited to grievances or complaints alleging harassment or discrimination, hearings involving academic freedom or tenure, allegations of professional misconduct, or student disciplinary hearings.

By weighing the costs of potential litigation against the cost of electronic discovery, the institution may decide to preserve all relevant data, to preserve reasonably accessible relevant data, or to forgo preservation altogether. In making this decision, keep in mind that failure to preserve potentially relevant data and documents could severely compromise the institution's legal position and result in court-issued sanctions and penalties.

Identifying Relevant Data

If the institution determines that data relating to a certain matter should be preserved, it should next identify the departments, employees, and other sources of data that are—or could be—affected. Since there are risks in failing to preserve and collect all potentially relevant data at the outset of a legal matter, it is advisable to make the preservation list overly inclusive. The preservation order can always be pared down to exclude people and sources who are not necessary to the investigation. To decide the proper scope of the preservation effort, the institution should use the following lists to closely examine anything that could be potentially relevant.

Where are the relevant people?

1. In specific departments
2. In administrative offices
3. Among academic administrators
4. On the faculty
5. On staff
6. Among the trustees
7. Among former employees or trustees

What are the relevant sources?

Electronic Files

1. Laptop/desktop computers
2. Smartphones, Blackberries, PDAs
3. Tablet devices
4. External storage media (diskettes, CDs, DVDs, thumb drives, flash drives, external hard drives)
5. Backup tapes/drives/servers
6. Shared network drives
7. SharePoint sites
8. Email servers
9. Voicemail/instant messaging/text messages
10. Audio/video tapes
11. Photographs/digital images
12. Internal/external websites including social networking sites, cloud storage areas

Paper Files

1. Desk drawers
2. Shared file cabinets
3. Personal file cabinets
4. Department file cabinets
5. Off-site storage
6. Home office files

The eTeam, possibly with assistance from outside counsel, should work with administrative, IT, and records management personnel to build a complete list of all people and data locations that fall within the preservation obligation.

Issuing a Preservation Directive

Legal counsel or a member of the eTeam should issue a preservation directive (sometimes called a litigation hold notice) to all identified individuals who may hold records relevant to the legal matter. The "Sample Preservation Directive" included in this toolkit can serve as a good starting point. At a minimum, the directive should:

- Inform the recipients of the institution's preservation obligations
- Identify, at the institution's discretion, the specific matter raising the duty
- Instruct recipients to think carefully about the manner in which their documents and data are created, maintained, stored, and accessed
- Require recipients to retain all potentially relevant records that are reasonably accessible
- Warn that noncompliance or lack of cooperation with individuals implementing the preservation directive is a serious offense that could lead to discipline up to termination
- Provide information on whom to contact if the recipient has questions or needs assistance

The preservation directive should be sent by hard copy and email with a request that each recipient sign and return it to the party issuing it. When senders deliver the directives by email, they should activate the tool that automatically confirms an email was delivered or read. In addition, a copy of each preservation directive should also be sent to the designated staff member in IT who will be assisting with the implementation of the directive.

IT Responsibilities

Upon receipt of a preservation directive, IT should stop its normal backup tape rotation, protect all backup media, and secure specific shared drives and data archives. In addition, IT should turn off any automatic deletions of emails and voice mails that may destroy or delete relevant information. Finally, IT should suspend any standard data deletion or hardware re-use practices for departing employees who are subject to a preservation directive.

IT personnel must interview each preservation directive recipient to gain additional information about potentially relevant data and to arrange for data collection. The "Script and Checklist for Data Custodian Interviews" on **page 8** of this toolkit can be very helpful to IT personnel in performing this task.

Ongoing Monitoring and Adjustments

During the course of litigation, recipients of the directive must preserve data created after the order was issued. If the litigation changes in scope, the institution might need to expand the reach of the directive or the number of people to whom the directive applies. In all cases, the institution should periodically issue a new or updated preservation directive to remind individuals of their obligations. In addition, legal counsel and IT should continue monitoring to ensure compliance.

After a lawsuit or legal matter has been resolved, counsel should notify the parties under the preservation directive, including IT and records management personnel, that the directive has been lifted, and they can resume their normal data management procedures.

Documenting Compliance

The institution should create and maintain a log of all preservation directives (P.D.) issued. The log should contain the following information about all outstanding directives:

- Subject of the matter
- Issuing officer
- Issue date
- Names and locations of recipients
- Date each recipient acknowledged receipt or opened directive

In addition, the institution should keep a file on each recipient of the preservation directive, and that file should be kept with the master file for the legal matter. The recipient's file should contain the information in the chart below and be maintained on a regular basis.

	Date P.D. Sent	Date P.D. Acknowledged	Date(s) P.D. Resent	Date Interviewed	Date P.D. Lifted
Custodian					

2. Sample Preservation Directive

[Letterhead of Issuing Officer]

To: [Distribution list, in the collective] OR [Each recipient listed individually]

From:[Issuing Officer]

[Date]

Subject: Preservation Directive—[Institution's] Duty to Preserve Data and Documents Relating to [Name of legal/investigative/etc.] Matter

PRIVILEGED AND CONFIDENTIAL

ATTORNEY-CLIENT COMMUNICATION

ATTORNEY WORK PRODUCT

The institution recently [received notice of/instituted] a [lawsuit/claim/dispute] regarding [insert brief description of the litigation/claim/dispute as understood by or known to employees]. The institution has a legal duty to preserve all data and documents in its possession that would be potentially relevant to this matter. The data and documents contained in the institution's files and computer systems will also be critical to our investigation into this matter and may be important sources of evidence. For these reasons, we require your assistance in preserving all data and documents in your files—or in those files you can access—that relate to this matter, as described below.

Directive Regarding Preservation of Data

Effective immediately, please preserve from deletion all data and documents—hard-copy documents and electronic documents—that pertain or relate in any way to [description of subject matter, key personnel, relevant time periods, etc.]. This includes:

- All communications by email and any other electronic means involving [subject matter, key players, witnesses, etc.]
- All information regarding [subject matter, opposing parties, products, key players]
- [Any additional categories of information likely to be relevant]

Destruction, alteration, deletion, and modification of such documents and data are strictly prohibited.

Failure to preserve relevant documents and data could result in significant penalties against [the institution].

2. Sample Preservation Directive *(continued)*

This Preservation Directive applies to paper documents as well as any electronic or magnetically stored data. When you are identifying and preserving electronic data, please keep in mind that "electronic data" includes, but is not limited to, the following:

1. All text files (including word processing documents, spreadsheets, and presentations)
2. Email
3. Files on shared servers
4. Files on email servers
5. Files on smartphones and hand-held devices (e.g. tablets)
6. Databases
7. Calendar entries
8. Computer system activity logs
9. Internet usage files
10. Backup tapes (if used for purposes other than disaster recovery)
11. Intranet or other internal network applications

At your individual work station, this directive requires you to preserve and retain all potentially relevant files stored on your hard drive and any system drives to which you have access. You must also preserve and retain all potentially relevant data on any laptop, home computer, handheld device, diskette, CD, DVD, "thumb" drive, voice mail, backup tape, videotape, or any other data storage medium.

To comply with this directive, you must immediately disable any functions that automatically delete or overwrite emails or other electronic data. Until further notice, the institution is suspending the sections of its regular record retention policy that require deletion or destruction of data.

[Institution may want to provide specific instructions on email retention, i.e., creation of a litigation folder.]

You will be advised when this preservation directive is no longer in effect.

Please contact [name] [department] if you need assistance or have any questions or concerns.

Thank you for your prompt and full compliance with this preservation directive.

3. Script and Checklist for Data Custodian Interviews

"Data custodians" are individuals who may possess records or documents that fall within the scope of an e-discovery preservation directive. IT and legal professionals need to interview all data custodians to ensure they do not miss any potentially relevant information within the scope of a preservation directive. This sample script and checklist provides guidance for IT professionals conducting these interviews.

Sample Greeting

Hello, my name is [name] and I am from [department] following up on the recent preservation directive concerning the [description of litigation/claim/dispute/investigation]. The purpose of this call is to find out if you have any relevant documents and ask a few questions about your document collection efforts.

Checklist

Questions	Response
1. Did you receive the preservation directive?	
2. Do you have any questions about the preservation directive?	
3. Have you located any hard copy documents covered by the preservation directive?	
a. If yes, can you describe those documents?	
b. How many?	
c. Are they separated from your other files?	
d. Do you continue to receive similar documents?	
e. Where do you look for documents? • Desk drawers • Onsite files • Other shared files • Stored files	

Checklist *(continued)*

Questions	Response
4. Have you located any electronic or computer files covered by the preservation directive? a. Email? • Inbox • Personal folders • Calendar • Journal • Sent items • Archive folders • Deleted items • Public folders	
b. Hand-held devices (smartphones, tablets, PDAs)	
c. MS Office? • Word files • Excel spreadsheets • PowerPoint presentations	
d. Other applications?	
e. Hard drive (including network and local hard drives)	
f. Diskettes, CD-ROM, DVD, or other external storage device	
5. Do you save files to the institution's network? a. My Documents b. Shared/departmental drives	
6. Do you personally create backups of your electronic records or files? a. Diskettes? b. CDs or DVDs? c. Any other location?	
7. Can you think of any other location to look for documents responsive to the preservation directive?	
8. Do you know anyone else who may have relevant documents but did not receive the preservation directive?	
9. Do you have any questions?	
10. As a final reminder, it is your responsibility to ensure that your relevant data and documents are not deleted. You will be advised by [the issuing officer] with further instructions.	

Sample Closing

Thank you for your time, and if you have any further comments or questions, please contact me at [phone number] or [email address].

4. Sample Data Collection Tracking Charts

Institutions that collect data in response to an e-discovery preservation directive or litigation hold need a way to track the data as it is collected, transferred, searched, and culled by attorneys and e-discovery vendors. Attorneys call this tracking form the "chain of custody" and use it to ensure data is not lost at any point along the e-discovery continuum. Chart 1 can be used to track all data identified as part of a preservation directive; the second chart only needs to be completed if a vendor is used to help the institution with e-discovery processes.

Chart 1

Privileged and Confidential Attorney Work Product

Name of Custodian	
Title/Position	
Office Location	
Date of Collection	
Name of Technician Collecting Data	
Description of Data (email, paper documents, electronic documents, other)	
Volume of Data (megabytes, gigabytes, etc.)	
Location of Data Collected (e.g., office file cabinet, email server, drive/file path)	
Notes	
Date Copied to Drive/Pulled	

Chart 2

Privileged and Confidential Attorney Work Product

Name of Custodian	
Date Delivered to Vendor	
Name of Vendor Recipient	
Date Uploaded/Imaged by Vendor	
Name of Technician Uploading/Imaging	
Date of Return to Custodian	
Name of Delivery Personnel	
Custodian Signature (when items are returned)	
Other changes in custody not noted above?	☐ Yes ☐ No If "Yes," describe in table below

Record of Additional Changes in Custody

From (name, company, title)	To (name, company, title)	Date	Reason

United Educators

EduRisk™ provides education-specific risk management resources to colleges and schools and is a benefit of membership with United Educators (UE). As a member-owned company, UE is committed to helping educational institutions by offering stable pricing, targeted insurance coverage, extensive risk management resources, and exceptional claims handling.

To learn more, please visit www.UE.org.