

GUIDELINES FOR ELECTRONIC DISCOVERY
AT THE
UNIVERSITY OF WASHINGTON

TABLE OF CONTENTS

A.	INTRODUCTION	1
B.	ELECTRONIC DISCOVERY COMMITTEE	1
C.	THE LANDSCAPE OF UNIVERSITY ELECTRONIC RECORDS SYSTEMS.....	2
1.	University Email Infrastructure	2
2.	Other University Email Storage Options	2
3.	Typical Email Use Patterns.....	2
4.	Storage of Other Electronic Records	3
5.	Disaster Recovery Processes.....	3
D.	EMPLOYEE RESPONSIBILITIES FOR RECORDS MANAGEMENT	3
1.	New Employees	3
2.	During Period of Employment.....	4
3.	Before Separating from Employment	4
4.	After Employee Separation.....	4
E.	NORMAL RECORDS RETENTION	5
F.	SPECIAL PRESERVATION OF RECORDS.....	5
1.	Document Preservation Plan.....	5
2.	Litigation Hold.....	6
3.	Duties of Persons Receiving a Litigation Hold.....	6
4.	Litigation: Actual or “Reasonably Anticipated”	7
5.	Ending Preservation Responsibilities	8
G.	RETRIEVAL OF ELECTRONIC RECORDS FOR DISCOVERY	8
1.	Options for Records Retrieval	8
2.	Factors to Consider in Records Retrieval	9
3.	Post-Retrieval Review	9
4.	Post-Production Duties	10
H.	OTHER GUIDANCE	10
	ATTACHMENT 1 – FLOW CHART	11
	ATTACHMENT 2 – FREQUENTLY ASKED QUESTIONS	12
	ATTACHMENT 3 – DOCUMENT PRESERVATION PLAN (SAMPLE)	16
	ATTACHMENT 4 – LITIGATION HOLD, KEY PROVISIONS	17
	ATTACHMENT 5 – COMPUTER SYSTEM CHECKLIST - ADMINISTRATOR	19
	ATTACHMENT 6 – COMPUTER SYSTEM CHECKLIST - INDIVIDUAL	20
	ATTACHMENT 7 – MAKING SECURE PRESERVATION COPIES	22
	ATTACHMENT 8 – STATEMENT OF COMPLIANCE	24

A. INTRODUCTION

Court decisions and rules now place substantial obligations on public and private organizations to (1) preserve all electronic materials that could be relevant to pending or anticipated lawsuits and (2) retrieve and produce such materials in the course of such litigation. These obligations also apply to the University of Washington. Failure to meet them may subject the University and the individuals involved to sanctions and liability.

The scope of these preservation and disclosure duties are broad. They apply to business-related electronic information wherever it is stored – at a University work station, on a laptop or PDA, and even at an employee’s home. The information at issue includes all forms of electronic communications and records such as email, word processing, calendars, voice messages, videos, photographs, and other digital information.

Although these legal duties require that information must be preserved, the preserved information need not be disclosed to the other party without first being appropriately reviewed to be sure that legally privileged information is removed. In other words, the University and its attorneys still can and will take steps to see that information that is legally protected will not be disclosed to the opposing party.

It is worth noting that the rules concerning preservation of hard copies of records have not changed. All printed documents under the control of involved individuals must also be preserved. Also, the new rules do not require the University to change any general records retention policies.

For more information, see the Frequently Asked Questions at Attachment 2.

B. ELECTRONIC DISCOVERY COMMITTEE

To help meet its obligations, the University created an Electronic Discovery Committee, made up of representatives from:

- The Attorney General’s Office
- Risk Management
- UW Technology
- Records Management Services
- The Public Records Office
- Human Resources
- Academic Personnel

As discussed below, this committee serves as a resource to help assure that the University’s approach to these issues is consistent and in compliance with applicable laws and University policies.

C. THE LANDSCAPE OF UNIVERSITY ELECTRONIC RECORDS SYSTEMS

1. University Email Infrastructure

The University of Washington is intentionally a very decentralized community – electronically and otherwise. With three campuses, dozens of schools, colleges, and research centers, largely-autonomous faculty, two hospitals and multiple clinics, many computing solutions have been developed independently to suit local needs. One aspect of this is that many departments and units operate their own independent email systems. So even though email infrastructure operated by the UW Technology Department accounts for a large portion of University email, there are many other email messages being sent from and delivered to servers managed and operated directly by colleges, schools, departments, and other administrative units, and by research projects within the University. In fact, at the time of this writing there are thousands of computers on the University network capable of receiving and storing email and approximately 200 different email servers that have been identified. These servers are, for the most part, operated by administrators using their own management practices.

2. Other University Email Storage Options

Although email comes into the University via central or departmental servers and often stays there until deleted, some people keep some or most of their email in “local folders” on their individual desktop or laptop or other “client machine.” In fact, email messages may be stored locally instead of – or in addition to – being kept on an email server.

3. Typical Email Use Patterns

The following are common ways that University faculty and staff handle their email.

- a. Centrally, where email inboxes and other folders are kept on a central (University/college/school/department/research group) server, with IT professionals maintaining the computers and backups.
- b. Centrally, then locally, where the email is initially sent to an Inbox on a central server, but is frequently or always pulled to a desktop/laptop/handheld and may be erased from the central server. In such cases the folders are usually or always stored on the desktop, laptop, or handheld
- c. Independently, where email comes directly to an inbox on an individually-managed computer, which stores the user’s folders.
- d. Off-Site, where all email for an individual is sent or forwarded to a non-University service (such as Yahoo, Google, etc.) or outside vendor.

The reality is that many individuals have “inherited”, rather than consciously chosen, one of the alternatives above and may not even realize how their email is handled. For example, a person could be downloading to their desktop and removing from the central

server and not realize it since they always use the same desktop to read and respond to email.

4. Storage of Other Electronic Records

In addition to emails, University faculty and staff create and use a myriad of other electronic materials ranging from traditional word-processing documents and spreadsheets to databases, digital images, audio, video, web pages, instant messages, blogs, calendars, technical drawings and more. While many records are stored on network servers that the University can monitor, individual users are often able to store them (or copy or move them) to individual desktop and portable devices that are beyond the University's field of observation or control. In some cases, University work products may be initially produced and stored on systems outside of University ownership and never touch University-owned equipment. Examples might include remote applications like Microsoft's "Office Live Workspace," a "Wiki" managed by another institution, or an email list archived by another institution.

5. Disaster Recovery Processes

Well-managed data systems at the University include a disaster recovery process that periodically copies its electronic data to tapes or other storage media so that the system and its contents can be restored in the event of an emergency. Many of these processes recycle the storage media on a very short cycle. For normal preservation purposes, emergency recovery copies of data are not practically accessible and interrupting their recycling would be impractical and expensive. As a result, such disaster recovery processes will usually be considered outside the scope of a Litigation Hold, unless otherwise directed. In contrast, other non-automated methods for archiving or backing up files are presumed subject to Litigation Holds. (For additional details, see the FAQs at Attachment 2.)

D. EMPLOYEE RESPONSIBILITIES FOR RECORDS MANAGEMENT

Each employee is individually responsible for handling and maintaining records (including University email and other electronic records) in accordance with University policy and management instructions. University managers, supervisors, and unit administrators are responsible for providing faculty, staff and other employees with appropriate access to such records and for overseeing the proper handling of records during employee transitions. The following outline provides additional information about these responsibilities:

1. New Employees

- a. In general, each new employee is set up with a "UW NetID" and provided with email, document, calendaring and other software, with appropriate rights to create, use, and modify University electronic records, as determined by University policies and the employee's manager.

- b. Employees should be informed of University policies regarding electronic records and reminded that all records relating to University business are the property of the University.

2. During Period of Employment

- a. Records Maintenance and Management - Each employee is required to maintain records he or she is responsible for in accordance with University and departmental records management policy and procedure.
- b. Records Retention - Records are to be retained according to the University Records Retention Schedules.
- c. Records Preservation - Upon receipt of a litigation hold or other instruction from University management, the employee is responsible for preserving the described records as instructed until notified otherwise.
- d. Records Production - Upon receipt of a request to find and produce records (for a public records request, litigation, or other reason), the employee is responsible for diligently searching for requested records and providing them to the designated University representative.

3. Before Separating from Employment

- a. Before an employee leaves a University position, the employee's manager, supervisor, or unit administrator is responsible for working with the employee to develop a plan for determining which employee maintained records should be preserved for business reasons or in accordance with University Records Retention Schedules and which records may be otherwise disposed of.
- b. The employee and manager, supervisor, or unit administrator are then responsible for arranging for the appropriate transfer and disposition of the records.

4. After Employee Separation

- a. Supervisors or administrators are responsible for managing records that are associated with a separated employee in accordance with UW policies and procedures.
- b. To allow time for the department to appropriately transfer ownership or dispose of the records, systems administrators must establish procedures to assure that email and other electronic records associated with a separated employee are not automatically deleted before the end of one year after the employee's separation.

E. NORMAL RECORDS RETENTION

As required by RCW 40.14, the University Records Management Services Office manages and oversees University compliance with state and federal laws and regulations relating to the preservation and destruction of electronic and paper information.

The Records Management Office works with the state to establish schedules for how long electronic and paper records and information must be retained. The office is responsible for developing Records Retention Schedules that identify records created or received by the University and specify how long those records must be retained. It is responsible for establishing standards, relating to University business requirements and needs, which ensure the legitimacy of University record-keeping systems. The program counsels and advises the University administration on the implementation of policy and procedure that promotes adherence to these standards and minimizes risk. It provides a wide range of services that are designed to help ensure the University is meeting its record-keeping responsibilities.

For more information, see the Records Management Office's website at <http://www.washington.edu/admin/recmgt/index.php>

F. SPECIAL PRESERVATION OF RECORDS

When a lawsuit is filed – or reasonably anticipated – the University has a duty to take special precautions to prevent the loss of potentially-relevant electronic data (as well as data on paper and in other forms.) Unless circumstances require a different approach, the following protocol will be followed to comply with these legal obligations.

1. Document Preservation Plan

When a lawsuit is commenced against the University – or information is received such that a lawsuit is reasonably anticipated – the lead unit (typically, Risk Management, Human Resources, or the UW Division of the Attorney General's Office) should develop a Preservation Plan outlining the immediate steps that need to be taken. The Plan (which could take the form provided in Attachment 3) should generally include some or all of the following basic steps:

- a. Identify the operating unit and individuals who might possess electronic data,
- b. Send a Litigation Hold to the appropriate individuals, and their supervisors and records coordinators, as appropriate,
- c. Identify a specific person to coordinate questions and responses.

Where the matter is complex or unusual, the following steps may also be considered:

- d. Gather a summary of the hardware and software involved. (The Computer System Checklists at Attachments 5 and 6 can be useful for this),
- e. Determine whether more aggressive steps (such as “imaging” or sequestering computers, stopping rotation of disaster recovery tapes, or taking snapshots of network folders) are warranted (See Attachment 7).

- f. Establish a method for following up, which may include sending out reminders, conducting preservation compliance checks, and addressing new questions or issues from agency employees with potential evidence.

In some instances, it may be useful to develop a written “Preservation Plan” outlining the steps that need to be taken. The plan (which could take the form provided in Attachment 3). The Electronic Discovery Committee may be consulted for assistance with any questions about an appropriate Preservation Plan.

2. Litigation Hold

A Litigation Hold will typically include:

- a. A definition of what constitutes a “record” and direct owners of potentially-relevant records to preserve them from destruction or modification (see Attachment 4).
- b. Direction to preserve relevant electronic and other pertinent records and general information on how to do so (which might include the checklist identified in Attachments 5 and 6). This may include directing the administrator(s) of relevant system(s) to avoid any centralized or automatic destruction or alteration of such records,
- c. Identification of the categories of information to be preserved,
- d. Contact information for the attorney(s), risk management professional, UW Technology or other IT professional, departmental lead, or any other contacts.

3. Duties of Persons Receiving a Litigation Hold

Receipt of a Litigation Hold does not necessarily mean the recipient is directly involved in the matter. Rather, it means the evidence which the University is obligated to preserve may be in the person’s possession or scope of responsibility and that the person, as an employee of the University, has a duty to preserve such information effective immediately. In particular, the person must:

- a. Suspend any University or divisional policies or procedures that might call for the routine destruction of electronic records under the recipient’s control.
- b. Discontinue personal practices regarding the destruction of electronic records. For example, the deletion of possibly-relevant emails, voice mails, drafts of documents, and the like must also be suspended.
- c. Disable any “janitorial” functions, such as the automatic deletion of emails or other electronic records. The designated computer support person should be immediately contacted if assistance is required to disable such functions.
- d. Protect and preserve all electronic records in their original electronic form, so that all information within it, whether visible or not is available for inspection. In other words, electronic records must be preserved, regardless of whether they have been reduced to a hard-copy or whether a hard-copy already exists.

- e. Protect and preserve any hard-copies of electronic records.
- f. Protect and preserve any new information that is generated or received that may be relevant to the litigation after receipt of a Litigation Hold.
- g. Advise the designated IT representative of any personal information that may potentially be affected by the Litigation Hold.
- h. Follow all other specific instructions in the Litigation Hold.
- i. Consult with the designated contact person regarding any questions involving electronic records.

4. Litigation: Actual or “Reasonably Anticipated”

The obligation to preserve evidence arises most commonly when a lawsuit has already been filed. However, the obligation can also arise when one knows—or should know—that future litigation is “reasonably likely.” Determining when facts or circumstances are reasonably likely to lead to litigation requires a case-by-case understanding of the facts and the application of experience and professional judgment.

The mere possibility of litigation does not necessarily mean it should be “reasonably anticipated.” Rather, a duty to preserve is triggered *only* when credible facts and circumstances indicate that a specific, predictable, and identifiable litigation is *likely*. Factors to consider in deciding whether litigation is “reasonably foreseeable” or “reasonably likely” may include, among other things:

- a. Historical Experience: Look at whether similar situations have led to litigation in the past.
- b. Filed Complaints: Be aware of complaints filed with the University or an enforcement agency, which may indicate a likelihood of future litigation.
- c. Significant Incidents: Pay attention to events resulting in known and significant injury.
- d. Attorney Statements: Examine any statements by an individual’s attorney regarding a dispute with the University.
- e. Employee Statements: Consider statements by University employees and officials regarding the potential of litigation.
- f. Initiation of Dispute Resolution Procedures: Give considerable weight to an action by a contractor to initiate a dispute resolution clause in a contract.
- g. Public Disclosure Requests: Consider whether a public disclosure request suggests the likelihood of future litigation. Although the University routinely gets thousands of public disclosure requests that are unrelated to litigation, some reasonably foreshadow a lawsuit.
- h. Significance of Dispute: The scale of a potential lawsuit may affect the trigger point for a litigation hold. For example, a higher degree of probability

might be appropriately required for a relatively small dispute versus one that poses the potential for large financial outlays or enterprise-wide impacts.

- i. Event Reported In the Press: Take stock of particularly bad events that are reported in the press, where history suggests litigation is likely.
- j. Common Sense: Use your powers of observation of human behavior and common sense. If an unfortunate or bad event occurs, especially if it is an unusual event or causes significant damage or distress, it may be reasonably anticipated that litigation will follow.
- k. Risks & Rewards: If the situation is uncertain, consider the relative costs of preservation against the likelihood of future litigation. Also consider the risks associated with the possibility of sanctions if preservation efforts are not undertaken.

5. Ending Preservation Responsibilities

When the litigation, or the threat of litigation, that prompted the Litigation Hold has ended, the person or unit issuing the Litigation Hold will inform those who received the notice that they are no longer under any special obligations to preserve the identified categories of materials. At that point, only the University's normal retention schedules will apply to the records. (The Office of Risk Management and the University's attorneys will be responsible for applying to their copies any special schedules for "litigation" records.)

G. RETRIEVAL OF ELECTRONIC RECORDS FOR DISCOVERY

In most cases, any need to actually produce preserved electronic records will come weeks or months after the preservation has occurred. When the University receives a request from an opposing party for production ("discovery") of electronic records, the University's counsel and primary University contact (Risk Management, Attorney General's Office or other unit) will determine the best approach to take in order to efficiently produce a complete and accurate response. The response may consist of any or all of the following: (1) supplying the requested information, (2) attempting to obtain a modification of the request (e.g., by narrowing the request's scope or obtaining agreement as to specific search terms), (3) declining to provide some or all of the requested data based upon expense of production, or other basis, (4) conferring with the Electronic Discovery Committee.

The Electronic Discovery Committee is available for consultation on such issues.

1. Options for Records Retrieval

Where some or all of the requested records must be retrieved, reviewed, and potentially disclosed, the following options should be considered to select the best approach to the specific request:

- a. Relying on the Computer User. In many instances, it is reasonable and sufficient to simply ask the computer user to identify, copy, and provide potentially-responsive electronic records and to certify that these steps have been taken. In these instances, the production of electronic data resembles the typical production of physical documents.
- b. Enlisting University Technical Support: Sometimes particular concerns about an individual user's time, skill, or dependability in identifying the universe of responsive records will warrant the direct involvement of the relevant system administrator or other University technical support personnel. Such personnel are often able to bring to bear sophisticated tools for searching and extracting large volumes of responsive records.
- c. Using Outside Consultants: Where identification or recovery of records requires technical expertise beyond that readily available from internal resources, an outside firm may be called upon for some or all of the work.

2. Factors to Consider in Records Retrieval

- a. Thoroughness: The approach in a specific case needs to be reasonably calculated to gather all potentially relevant records.
- b. Operational Efficiencies: The activities required should be operationally efficient to ensure timely preservation and processing of the data.
- c. Individual Privacy: The processes implemented to respond to electronic discovery should take into account personal privacy concerns.
- d. Risk of Data Loss: Reasonable steps will be needed to protect data from loss through inadvertent or intentional deletion of files or loss of data storage media.
- e. Individual Disruption: Procedures should take account of the potentially significant impacts in terms of time and distraction for individuals named in the lawsuit.
- f. Procedural Consistency: While the appropriateness of some procedures may vary depending on the circumstances of the case, once a process has been adopted, it should be consistently followed and executed.

3. Post-Retrieval Review

As potentially-responsive electronic records are gathered, University attorneys will review the retrieved data for legal relevance and privilege or other protected status, and will handle all formal and informal responses to the discovery requests.

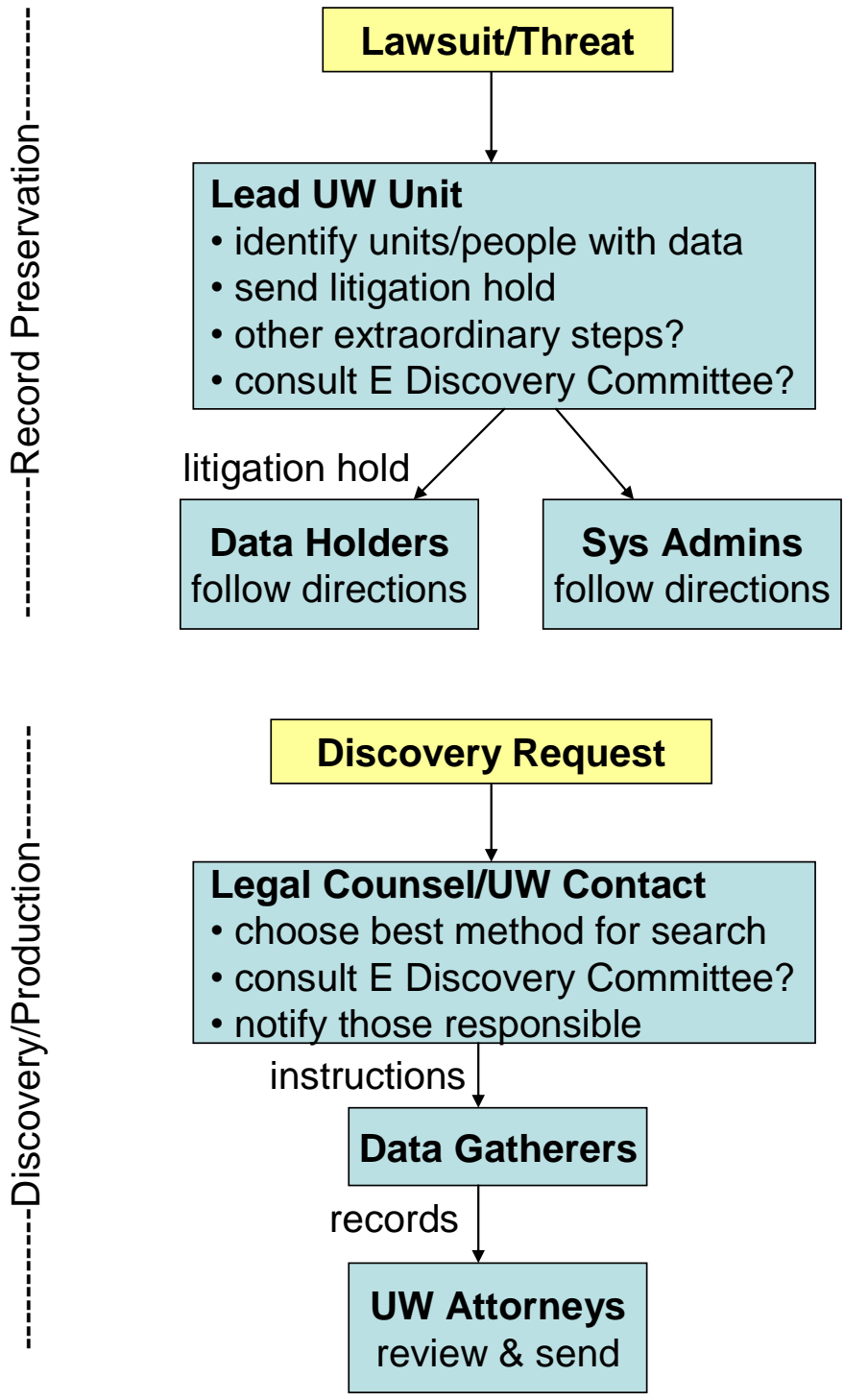
4. Post-Production Duties

The duty to preserve and produce information related to a lawsuit does not end with an initial production of records. Relevant information and records generated after the Litigation Hold must be preserved for future retrieval as the lawsuit progresses.

H. OTHER GUIDANCE

This handbook is intended to be a resource for the University community as it develops and implements best practices to comply with the obligations now placed on it by court decisions and rules. In addition to the preceding discussion and the following attachments, the Electronic Discovery Committee should be consulted on any questions with respect to the content of this handbook and for further discussion of appropriate handling of specific circumstances where document preservation or retrieval may be required.

ATTACHMENT 1 – FLOW CHART



ATTACHMENT 2 – FREQUENTLY ASKED QUESTIONS

1. What do “electronic discovery” and “data preservation” mean?

“Discovery” is the process by which relevant information is gathered by the parties in a lawsuit. One of the ways a party to a lawsuit can obtain “discovery” of relevant information is by asking other individuals or entities to produce documents. Federal and state courts have long recognized that the term “documents” includes electronic data and that electronic data are thus subject to the same discovery rules as other evidence relevant to a lawsuit. The issue has received substantial national attention recently, however, because of a series of court rulings resulting in the imposition of huge sanctions on parties for their failure to preserve electronic data and because of amendments to the Federal Rules of Civil Procedure that took effect on December 1, 2006. Upon notice that a lawsuit has been commenced against the University (or a charge filed with an administrative agency), or if it is reasonably anticipated that a lawsuit may be brought (or a charge filed), the University and all of its faculty and staff members are under a legal duty to preserve all evidence, whether hard copy or electronic, that might be relevant to the lawsuit.

2. What data needs to be preserved?

The new federal rules require a party to suspend routine or intentional purging, overwriting, re-using, deleting, or any other destruction of electronic information relevant to a lawsuit, wherever it is stored – at a University work station, on a laptop, or cellular phone, or at an employee’s home. It includes all forms of electronic communications, e.g., email, word processing documents, calendars, voice messages, instant messages, spreadsheets, SharePoint files, Wiki materials, videos or photographs. This electronic information must be preserved so that it can be retrieved – if necessary – at a later time. The information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection – i.e., it is not always sufficient to make a hard copy of electronic communication.

3. What will I have to do?

You will be notified of the duty to preserve electronically stored information through a notice called a “litigation hold” or “preservation hold.” You will then be asked to cooperate with the Attorney General’s Office, the Office of Risk Management, and/or University IT personnel to ensure that we identify and preserve all potential sources of electronically stored information (ESI) in your possession or under your control. You may be asked to complete and return a questionnaire identifying all potential sources of ESI. If so, it is critical that you complete and return the questionnaire without delay. You may also be asked to complete a signed statement confirming that you have completed the required search and retention as requested. Until IT personnel have taken steps to preserve your ESI, you should be particularly careful not to delete, destroy, purge, overwrite, or otherwise modify existing ESI.

4. How long will this go on?

The University's counsel and/or primary University contact (Risk Management, Human Resources or other unit) will advise you when you and the University are no longer obligated to retain the preserved data. Generally, this will be when the statute of limitations has expired with respect to the claim or – if litigation has been commenced – when the lawsuit and all appeals have been concluded. When the duty to preserve evidence ends, the preserved data will be returned to you or destroyed, at your option and in accordance with records management schedules. If at any time you question whether to continue retaining the records, you need to contact the appropriate contact person listed in the Litigation Hold communication before destroying any documents.

5. Do I need to also preserve data on my home computer?

The same rules apply to any computer that stores information potentially relevant to a lawsuit involving the University. Thus, if you use your home computer for University-related business (including email on your University email account or on a personal account such as AOL, gMail, etc.), you must preserve the data on that computer.

6. Can I take personal or sensitive material that isn't relevant to the case off my computer?

You may remove data from your computer (or segregate it from the data that will be preserved) if you are absolutely certain that it is unrelated to the claim (e.g., on your home computer correspondence entirely unrelated to University employees or University business, income tax returns, your music library, etc.). However, we often find that it is difficult at the beginning of a lawsuit to be certain about what might later turn out to be relevant. So you should examine each and every file you are considering deleting – i.e., do not make wholesale deletions of data. You may be questioned under oath at a later date by an attorney representing the opposing party about what data you may have destroyed.

7. I previously deleted something that might be relevant – should I be concerned about that?

The duty to preserve information arises only when there is a reasonable anticipation of litigation. Electronically stored information deleted before that time pursuant to retention policies, should not create a problem.

8. What if I am involved in an ongoing matter relating to the person who is suing the University?

You must also preserve any new electronic information that is generated after receipt of a litigation hold that may be relevant to the dispute (such as an employment claim by a current employee where relevant new documents may be created during the ongoing employment relationship).

9. Who is going to be paying for the cost of preserving electronic records?

Most external costs (such as IT consultants) associated with complying with the electronic discovery requirements will be handled in the same manner as other litigation expenses are presently handled. Internal costs (time spent by University staff members, applicable storage costs and the like) will be absorbed by the department.

10. Who will be looking at my University data?

This depends on the reason for the Litigation Hold. If the matter involves a complaint or claim that requires investigation, appropriate University personnel from departments such as the Office of Risk Management, Human Resources, Labor Relations, the Attorney General's Office, and perhaps others may be reviewing your records in the course of the investigation.

In other cases, it may be that no one will initially review your records until and if there is a lawsuit filed with discovery requests made.

11. Who decides what data will be turned over to the opposing party?

The University, as owner of the data, will make these decisions based on advice from its attorneys. Before any data is turned over to the opposing party, the University's attorneys will review it for relevance and confirm it is not otherwise protected or privileged.

12. Since when did we have to go to all this trouble?

Electronically stored information has been discoverable since the 1980's. Because of the egregious misconduct by several organizations and because of the ever-widening use of computers, over the last several years the courts have developed rules specific to the preservation of electronic data. The new amendments to the Federal Rules of Civil Procedure addressing electronic discovery took effect December 1, 2006.

13. What if I don't want to disclose my University data?

The University and its employees have a legal duty to preserve, and subject to the rules governing discovery, turn over electronically stored information. In short, the law does not offer us a choice. Failure to abide by the law may result in judicially imposed monetary (or other) sanctions against the University and/or you individually and adverse findings in the litigation. We will take steps to protect your privacy and to ensure that protected/privileged information is not disclosed, but ultimately the court will be the arbiter of whether sensitive information must be disclosed.

14. What should I do with my electronic data if I leave the University?

If you plan to leave your employment with the University during the pendency of a lawsuit for which you have received a preservation hold, you should confer with the Attorney General’s Office and other contacts listed in the Litigation Hold notice.

15. What if I have additional questions?

Get in touch with the University’s counsel and/or primary University contact (Risk Management, Human Resources or other unit) contacts listed in the Litigation Hold notice.

16. Do Litigation Holds apply to back-up systems?

Systems administrators and computer users at the University may mean two different things when they refer to “back-up” systems for electronic records. They are distinguished below as “Disaster Recovery” systems and “Records Preservation & Archiving” systems. The objectives and features of each type are discussed below, as are the general expectations concerning the application of Litigation Holds.

Type of System	Objectives	Features
Disaster Recovery	<ul style="list-style-type: none"> • To serve as a “safety net” to enable immediate restoration of file structure and content in case of system “crash” 	<ul style="list-style-type: none"> • An automated system copies files to high capacity tapes or other media on at least a daily basis • Copies are stored off-site, as well as locally for quick recovery after an incident • No long-term storage (media are regularly “written over”) • Not generally within Litigation Holds
Records Preservation & Archiving	<p>Some or all of the following:</p> <ul style="list-style-type: none"> • To provide high-security by taking sensitive records “off-line” • To preserve storage space by taking older records “off-line” • To provide stable long-term preservation of important records 	<ul style="list-style-type: none"> • Ad hoc or variable schedule, depending on purpose • Software and media highly variable • Media may or may not be kept off-site • Storage media may or may not be overwritten • For purposes of electronic discovery, copies of records made for this purpose are generally no different from other records • Generally are within the scope of Litigation Holds

ATTACHMENT 4 – LITIGATION HOLD, KEY PROVISIONS

A Litigation Hold should generally contain the following provisions, either incorporated in the body of a letter or memo or as an attachment.

[Description or reference to description of Matter]

To prepare for the defense of the actual or potential litigation described, the University may need access to a complete copy of all documents that could reasonably relate to this matter. These documents may reside in your office, your home, may be held in the University Records Center and/or University Archives, or may exist in other places.

“DOCUMENT” INCLUDES A WIDE VARIETY OF RECORDS AND MATERIALS.

Be aware that “document” typically is broadly defined by courts to include, among other things:

- writings
- emails
- drawings
- graphics
- charts
- photographs
- phone records
- images
- all electronically-stored information, and
- any other data compilations from which information can be obtained.

DO NOT DESTROY, DELETE OR DAMAGE ANY DOCUMENTS THAT MAY RELATE IN ANY WAY TO THIS MATTER.

It is important that all potentially relevant documents in your possession and in the possession of the University be retained, preserving as well the original format, if feasible. In addition, if you are aware of other documents that may be relevant but which you do not currently have access to, please so inform _____. In addition, please suspend any scheduled destruction, archiving, or deletion of documents related to this matter until you specifically have been advised that you are authorized to do so. Failure to comply with any of the above could result in penalties imposed upon the University and/or you by a court.

INCLUDE EVERYTHING REASONABLY RELATING TO THIS MATTER.

Since it is early in this matter, it is difficult to determine what information may or may not be relevant. However, at a minimum, you should retain the originals and copies of any and all documents (including emails and electronically stored documents) that you may have in your possession that: (1) were sent to or from _____, (2) refer to _____ by name,

title, or implication, (3) relate to any employees in _____'s work group and managers and/or discuss their duties and performance, (4) relate in any manner to _____'s performance or (termination), including to any event in which _____ was investigated, disciplined or counseled, (add other matters pertinent to case).

If you have any doubt as to whether a document might be relevant, retain it. Do not delete or dispose of it. You should retain the documents in a place where they can be easily located upon request. Please do not hesitate to communicate with _____ if you have any questions.

Since "documents" include existing documents, as well as documents that may be created in the future, you also should provide this office with documents created after your receipt of this letter.

IF YOU HAVE QUESTIONS ABOUT THESE INSTRUCTIONS, CONTACT ONE OF THE FOLLOWING INDIVIDUALS

ATTACHMENT 5 – COMPUTER SYSTEM CHECKLIST - ADMINISTRATOR

The checklist below may be of use to systems administrators as they determine potential locations of electronically stored information (ESI) that might assist the University in responding to a potential or existing lawsuit.

ESI Locations:

_____ **Servers**

Describe each server or server cluster: what kind, their purpose, and how many.

_____ **Mainframes**

Describe what kind, their purpose, how many

_____ **Digital printers, copiers, scanners**

List any devices in which ESI gets stored in scanning directories and does not get saved to the main server directory)

_____ **Sharepoint, Wiki, or Blog Sites**

List employee chat rooms or collaborative space where work is conducted or conversations occur

_____ **Password Protected Internet Sites**

List any sites used by employees who work with outside consultants through a password protected internet site

_____ **Backup Tapes**

_____ **Text or Instant Messaging**

List any applications that enable employees to send “text or instant messages”

_____ **Databases**

List any databases and indicate what, when, where and how many

_____ **Email lists**

Specify any email lists (what, when and who is on it)

_____ **Metadata Scrubbing Software**

Indicate if you use this type of software on any of your storage

_____ **Media Cards**

_____ **RFID Readers (Radio Frequency Identification Device)**

_____ **Laptops**

_____ **Desktops**

_____ **PDA's**

Notes: Please provide any additional information you think would be helpful in understanding your Electronically Stored Information file types and locations.

ATTACHMENT 6 – COMPUTER SYSTEM CHECKLIST - INDIVIDUAL

The checklist below may be of use to individuals as they determine potential locations of electronically stored information (ESI) that might assist the University in responding to a potential or existing lawsuit.

1. Computers

Please identify computer systems (including home computers, laptops, blackberry, personal digital assistants) you use to conduct University business.

For each computer system that you use, please answer the following. For “Name” please enter a unique designation which will allow you to distinguish this system from the others that you use. If you are sure that a given system has no information related to your position at the University, you do not need to list it.

No.	Name	Type Laptop, Desktop, PDA, etc.	Ownership University or personal?	Location of Use Home, office, travel, all?
1				
2				
3				
4				

2. Data storage

Besides the internal hard disk(s) in the above systems(s), please list the other places where you store electronic data related to your position at the University. Note that backups are treated separately in the next section. If a data store is associated with one of the computers listed above, please enter that system’s number as listed in the first column above.

Name	Type File Server, External Drive, Flash Drive, DVD, CD, Tape, Diskette?	Purchase \$ University \$ or personal \$?	Location of Use Home, office, travel, all?	Computer No.

3. Backups

Please state how the backups are completed for each system listed above.

Computer No.	Type and Location Departmental Network Backup, Local Tape, Local DVD, etc.?	Schedule for Backup Daily, weekly, irregularly?

4. Mail service

List the email service(s) on which you send or receive University-related messages. If you store messages on a local computer, give the associated system number(s).

Service University email Service, Department mail Service, MSN, AOL, Yahoo, etc.	Use Work, personal, or both?	Messages Stored Locally? on Computer No.

5. Collaborative work

List any Web pages, email lists, blogs, wikis, or other collaborative environments you participate in for University work.

Collaborative system Wiki, Sharepoint, Web server,	Location URL, archives, etc.	Purpose

6. Your primary computer support person/group

Complete the contact information for the individual or group that provide your computing and networking support.

Name _____

Email address _____

Phone number _____

Employee Signature _____

ATTACHMENT 7 – MAKING SECURE PRESERVATION COPIES

UW Technology and other system administrators at the University have technical tools that permit them to copy and securely preserve entire sets of electronic records. Such actions can include:

- copying the entire network server contents of a user’s email account or document folders (sometimes referred to as taking a “snapshot” of such an account) and
- copying (or “imaging”) the contents of a user’s individual computer

Such copies may then be stored on a disk or on a secure server location and can provide a complete picture of those segments of the user’s electronic records as of the time the copy was made.

1. When is it appropriate to make a secure preservation copy of records?

When the University is obligated to or desires to protect a set of electronic records that may be subject to a public records request or is reasonably believed to be relevant to current or anticipated litigation, making a secure preservation copy can be a useful supplement to a litigation hold. However, because such actions are generally not necessary and because doing so for every records request or potential lawsuit would impose significant burdens on the University (staff time, storage costs, employee relations, etc.), making secure preservation copies is appropriate only where (a) there is unusual risk to the integrity of the records or (b) the University and individual user agree that making a secure preservation copy would be convenient.

a. Risk to Integrity of Records

University management may make a secure preservation copy of electronic records whenever there is a reasonable basis to believe that the integrity of the records would otherwise be at abnormally high risk. Examples of circumstances warranting such action would include:

- the account or computer is known to contain records with an exceptional value to the University
- the form or location of the records makes them unusually volatile
- the records are subject to the operation of an automated system that may otherwise dispose of them
- there is reasonable suspicion or plausible allegations that the user or another person with access to the user’s network account or computer may delete or alter the records

b. Mutual Convenience

Sometimes the University and a specific user will wish to make a secure preservation copy of records:

- (1) in order to facilitate a search for records or
- (2) in order to eliminate any subsequent allegation that the user deleted or modified records.

Making such a copy may be appropriate for either or both these purposes after discussion with the user. In considering making such a copy for the mutual convenience of the user and the University, one should recognize that any substantial delay in making the copy will diminish the potential value of the copy in eliminating accusations of deletion or modification of records.

2. When, if at all, should a user be informed that a secure preservation copy is being made?

When the reason for making a secure preservation copy is management's concern that the integrity of the records may be compromised by someone with access to them, neither the user or others with access to the account or computer should be informed in advance. Whether the user is informed after records have been copied will depend on the matter involved, the nature of the records, and the user's duties and relationship to the records.

3. Who has authority to direct the making of a secure preservation copy?

University management should make a secure preservation copy of records when authorized or directed by an assistant attorney general, the Office of Risk Management or a supervisor in the user's chain of command.

ATTACHMENT 8 – STATEMENT OF COMPLIANCE

**THIS DOCUMENT IS PROVIDED UNDER THE ATTORNEY-CLIENT PRIVILEGE
AND SHOULD BE CONSIDERED CONFIDENTIAL**

I was assigned responsibility by the University of Washington to search for specified documents on behalf of the agency pertinent to [INSERT CASE NAME].

In accordance with instructions, procedures, and directions received from the representative of the University’s legal team, I conducted a diligent and good faith search of the files and records of my unit and/or directed others to do the same.

To the best of my knowledge, information and belief, all existing documents maintained in University files in the ordinary course of business that are responsive to the requests for production have been provided to the representative of the University’s legal team. I am aware of no documents in University files that are responsive that have not been thus provided, and I have no reason to believe that any such documents exist.

DATED this _____ day of _____, [year].

Signature

Print Name

Telephone; Address

University of Washington

Files For Which I Was Assigned Search
Responsibility

Others Who Assisted:

