



REED COLLEGE
eDISCOVERY GUIDELINES
FOR
PRESERVATION AND PRODUCTION
OF ELECTRONIC RECORDS

Revised 1-2-12

TABLE OF CONTENTS

A. INTRODUCTION	1
B. THE LANDSCAPE OF ELECTRONIC RECORDS SYSTEMS	1
1. Email Infrastructure	1
2. Email Storage Options	1
3. Email Use Patterns	2
4. Storage of Other Electronic Records	2
5. Disaster Recovery Systems.....	2
C. SPECIAL PRESERVATION OF RECORDS	2
1. Document Preservation Plan.....	2
2. Litigation Hold.....	3
3. Duties of Persons Receiving a Litigation Hold.....	4
4. Litigation: Actual or “Reasonably Anticipated”	4
5. Ending Preservation Responsibilities	5
D. RETRIEVAL OF ELECTRONIC RECORDS FOR DISCOVERY	5
1. Options for Records Retrieval	6
2. Factors to Consider in Records Retrieval	6
3. Post-Retrieval Review	7
4. Post-Production Duties	7
Appendix 1 – FLOW CHART OF eDISCOVERY PROCESS.....	8
Appendix 2 – FREQUENTLY ASKED QUESTIONS	9
Appendix 3 – DOCUMENT PRESERVATION PLAN (SAMPLE)	12
Appendix 4 – LITIGATION HOLD, KEY PROVISIONS	13
Appendix 5 – COMPUTER SYSTEM CHECKLIST - ADMINISTRATOR.....	15
Appendix 6 – COMPUTER SYSTEM CHECKLIST - INDIVIDUAL	16
Appendix 7 – STATEMENT OF COMPLIANCE.....	18

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 apply to Reed College. Failure to meet them may subject the College 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 – on a College computer, on a laptop or handheld device, and even at an employee’s home. The information at issue includes all forms of electronic materials such as email, word processing documents, calendars, voice messages, images, videos, and other digital information.

Although legal duties require that information must be preserved, the preserved information need not be disclosed to the opponents without first being appropriately reviewed to be sure that legally privileged information is removed. In other words, the College and its attorneys 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 College to change any general records retention policies.

For more information, see Appendix 1(Flow Chart of eDiscovery Process) and Appendix 2 (Frequently Asked Questions).

B. THE LANDSCAPE OF ELECTRONIC RECORDS SYSTEMS

1. Email Infrastructure

Reed College has a highly centralized email infrastructure. All messages addressed to user@reed.edu are processed by a unified system managed by staff in Computing & Information Services (CIS).

2. Email Storage Options

Although email comes into the College via central servers and often stays there until deleted, some people keep much of their email in “local folders” on their individual desktop or laptop computer. Email messages may be stored locally in addition to being kept on the central email server.

3. Email Use Patterns

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

- a. Centrally, where email inboxes and other folders are kept primarily on a central server, with CIS staff maintaining the server and backups.
- b. Centrally, then locally, where email is initially sent to an Inbox on the central server but is copied to a desktop/laptop/handheld device and erased from the central server. In such cases the folders are usually or always stored on the desktop, laptop, or handheld device.
- c. Off-Site, where all email for an individual is immediately forwarded to a non-College service (such as Yahoo, Google, etc.) or other outside vendor.

The reality is that many individuals may not even realize how or where their email is stored. For example, copies of Inbox messages may be "cached" on a local computer without the individual realizing it.

4. Storage of Other Electronic Records

In addition to emails, College faculty and staff create and use many other electronic materials ranging from word-processing documents and spreadsheets to databases, digital images, audio, video, web pages, text messages, blogs, calendars, and more. While many records are stored on network servers managed by CIS, individual users sometimes store them (or copy or move them) to individual desktop and portable devices.

5. Disaster Recovery Systems

Most College servers are backed up to tape or other storage media to enable the server and its contents to be restored in the event of an emergency. Retention periods for data on backup systems vary, as described in the *CIS Electronic Data Backup and Retention Policy*. See: http://web.reed.edu/cis/policies/data_storage.html

C. SPECIAL PRESERVATION OF RECORDS

When a lawsuit is filed – or reasonably anticipated – the College has a duty to take special precautions to prevent the loss of potentially-relevant electronic data. 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 College — or information is received such that a lawsuit is reasonably anticipated — the Vice President/Treasurer's Office, in consultation with legal counsel, the Human Resources Office, Computing & Information Services, and others as appropriate, will develop a *Preservation Plan* outlining the

immediate steps that need to be taken. The plan (which could take the form provided in Appendix 3) should generally include some or all of the following basic steps:

- a. Work with College Counsel and Plaintiff Counsel to define parameters for relevant electronic data. Such parameters may include the starting date (or time period) within which electronic materials may be deemed relevant; the specific categories of electronic materials to be included in a search process; and the criteria for conducting a document search (e.g., in the case of email the sender and/or recipient; in the case of email or other documents, one or more character strings to be matched, etc).
- b. Identify the departments and individuals who might possess relevant electronic data,
- c. Send a Litigation Hold to the appropriate individuals,
- d. Designate a specific person to coordinate and serve as a contact.

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 Appendix 5 and 6 can be used 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.
- 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.

2. Litigation Hold

A Litigation Hold will typically include:

- (a) A description of potentially relevant documents, directing owners of such materials to preserve them from destruction or modification (see Appendix 4);
- (b) Direction to preserve relevant electronic records and information on how to do so (which might include the checklist identified in Appendix 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) Identification of the date range applicable to document that need to be preserved;

- (e) Contact information for College Counsel, CIS representative, departmental head, or any other relevant 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 College is obligated to preserve may be in the person's possession or scope of responsibility and that the person, as an employee of the College, has a duty to preserve such information effective immediately.

In particular, the person must:

- a. Suspend any College 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 CIS 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 CIS 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 College 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 College.
- e. Employee Statements: Consider statements by College 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. Common Sense: Use your powers of 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.
- h. 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 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 College’s normal retention schedules will apply to the records.

D. 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 College receives a request from an opposing party for production (“discovery”) of electronic records, College Counsel 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) or declining to provide some or all of the requested data based upon expense of production, or other basis.

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 CIS 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 CIS staff. Such staff are often able to provide sophisticated tools for searching and extracting large volumes data.
- 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.

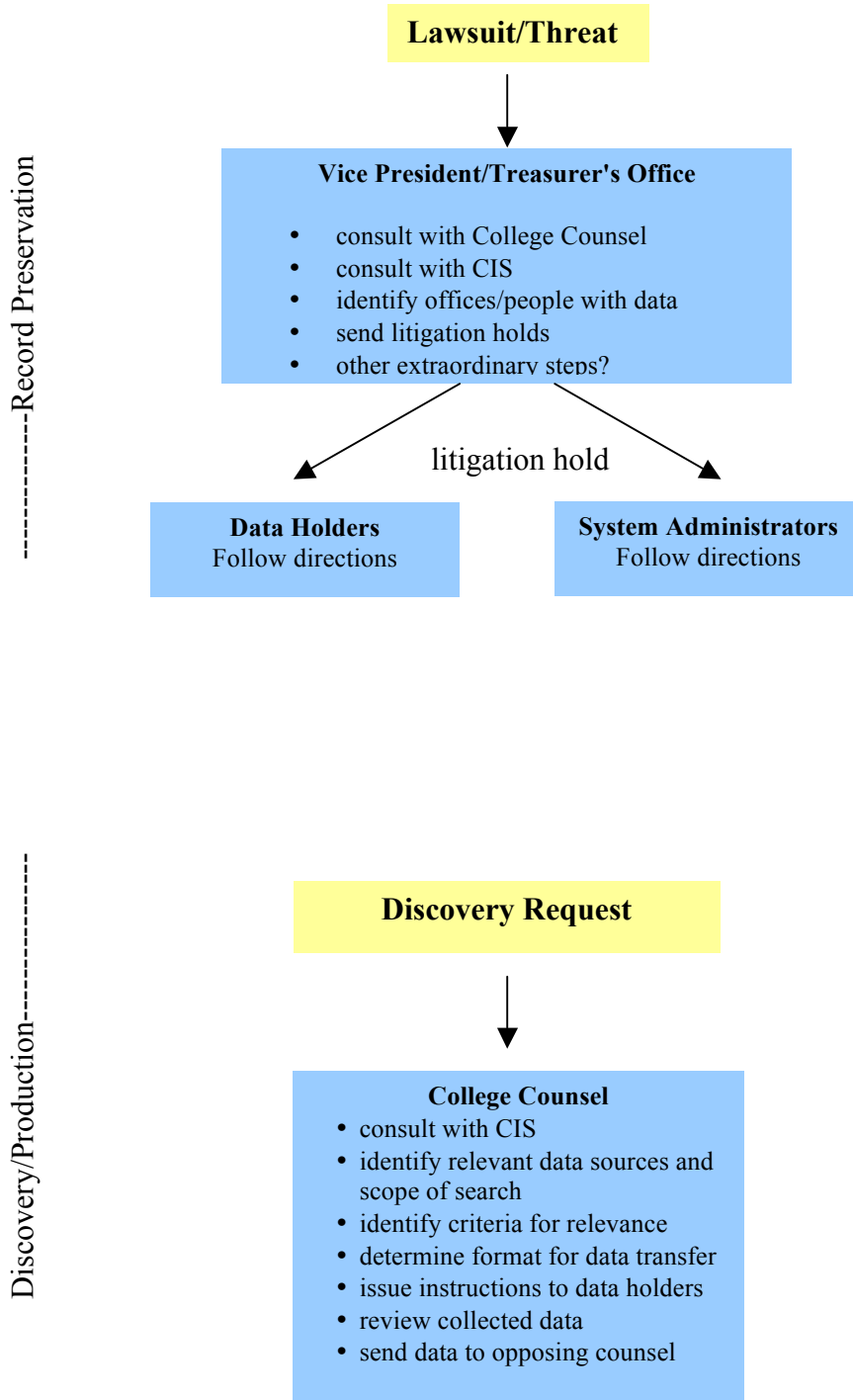
3. Post-Retrieval Review

As potentially-responsive electronic records are gathered, College Counsel 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.

Appendix 1 – FLOW CHART OF eDISCOVERY PROCESS



Appendix 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 College (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 College 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 need 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 – on a College computer, on a laptop, on a cellular phone or other handheld device, 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, 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 College Counsel, CIS staff, the Human Resources Office, or others 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 CIS staff 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 College's counsel and/or primary College contact (Human Resources, CIS, or other office) will advise you when you and the College 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 College. Thus, if you use a personally owned computer for College-related business 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., correspondence entirely unrelated to College employees or College business, such as income tax returns, your music library, etc.). However, 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 College?

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).

10. Who will be looking at my College data?

This depends on the reason for the Litigation Hold. If the matter involves a complaint or claim that requires investigation, College Counsel and appropriate College staff from Human Resources and perhaps other offices 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 College, 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 College'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 College data?

The College 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 College 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 College?

If you plan to leave your employment with the College during the pendency of a lawsuit for which you have received a preservation hold, you should confer with College Counsel, CIS, and other contacts listed in the Litigation Hold notice.

15. What if I have additional questions?

Get in touch with the College's counsel and/or primary College contact (Human Resources or other department) contacts listed in the Litigation Hold notice.

Appendix 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 College 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 College Records Center and/or College 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 College 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 College 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 department 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

Appendix 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 College in responding to a potential or existing lawsuit.

ESI Locations:

___ **Servers**

Describe each server or server cluster: what kind, their purpose, and 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)

___ **Wiki, Forum, or Blogs Hosted by Reed**

List employee collaborative spaces 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 Media**

___ **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**

___ **PDAs**

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

Appendix 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 College in responding to a potential or existing lawsuit.

1. Computers

Please identify computer systems (including home computers, laptops, handheld devices, etc.) you use to conduct College 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 College, you do not need to list it.

No.	Name	Type Laptop, Desktop, PDA, etc.	Ownership College 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 College. 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?	College or personal equipment?	Location of Use Home, office, travel, all?	Computer Serial 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 College-related messages. If you store messages on a local computer, give the associated system number(s).

Service College email service, External service (Gmail, 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 College work.

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

Employee Signature _____

Appendix 7 – STATEMENT OF COMPLIANCE

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

I was assigned responsibility by Reed College 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 College’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 College files in the ordinary course of business that are responsive to the requests for production have been provided to the representative of the College’s legal team. I am aware of no documents in College 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	<u>Others Who Assisted:</u>
_____ Print Name	_____
_____	_____
_____ Telephone; Address	_____
_____ Reed College	_____

Files For Which I Was Assigned Search Responsibility: *(file names or description of file range)*

_____	_____
_____	_____
_____	_____
_____	_____