PROCEDURE 4040P
Community Relations

PRESERVATION AND PRODUCTION OF ELECTRONIC RECORDS

Electronic Discovery Committee

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

- The Attorney General's Office
- WSD Risk Management
- Information Technology
- Assistant Superintendent
- The Public Records Office
- The Superintendent and/or Director of Human Resources, as appropriate

As discussed below, this committee will serve as a resource to assist the WSD's management of these issues consistent with applicable laws and WSD policies.

WSD Electronic Record Systems

When the WSD determines that there is a reasonable anticipation of litigation, responsive electronic records may include email generated or retained by WSD employees, whether maintained on the WSD servers or copied 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.

In addition to emails, WSD 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 WSD 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 WSD's field of observation or control.

The WSD maintains a system of tapes or other storage media that periodically copy the system's data to enable the system and its contents to be restored in the event of an emergency. This backup system recycles the storage tapes on a regular basis. 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 systems will usually be considered outside the scope of a Notice of Records Preservation, unless otherwise directed.

As required by RCW 40.14.040, the WSD Records Officer manages and oversees WSD compliance with state and federal laws and regulations relating to the preservation and destruction of electronic and paper information.

Special Preservation of Records
When a lawsuit is filed – or reasonably anticipated – the WSD must take special precautions to prevent the loss of potentially-relevant electronic data. Unless circumstances require a different approach, the following protocol will be followed.

Document Preservation Plan
When a lawsuit is commenced against the WSD – or information is received such that a lawsuit is reasonably anticipated – the lead unit (typically, Risk Management, Human Resources, or the Assistant Attorney General assigned to the WSD) 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 steps:

- Identify the operating unit and individuals who might possess potentially relevant electronic data;
- Send a Litigation Hold to the individuals identified; and
- 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:
- Gather a summary of the hardware and software involved. (The Computer System Checklists at Attachment 5 and 6 can be useful for this),
- 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.
- 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.

The Electronic Discovery Committee should be consulted for assistance with any questions about an appropriate Preservation Plan.

Litigation Hold
A Litigation Hold will typically include:

- A definition of what constitutes a “record” and direct owners of potentially-relevant records to preserve them from destruction or modification (see Attachment 3).
- Direction to preserve relevant electronic records and general information on how to do so (which might include the checklist identified in Attachment 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,

- Identification of the categories of information to be preserved,
- Contact information for the attorney(s), risk management professional, WSD Technology or other IT professional, and any other contacts.

Responsibility 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 potential evidence which the WSD must preserve may be in the person's possession or scope of responsibility and that the person, as an employee of the WSD, has must immediately take reasonable steps to preserve such information. In particular, the person must:

- Suspend any WSD or divisional policies or procedures that might call for the routine destruction of electronic records under the recipient's control.
- Discontinue personal practices regarding the deletion of electronic records. For example, the deletion of possibly-relevant emails, voice mails, drafts of documents, and the like must also be suspended.
- 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.
- Protect and preserve all potentially relevant 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 also been reduced to a hard-copy or whether a hard-copy already exists.
- Protect and preserve any hard-copies of electronic records.
- Protect and preserve any new documents that are generated or received that may be relevant to the litigation after receipt of a Litigation Hold.
- Advise the designated IT representative of any personal information that may potentially be affected by the Litigation Hold.
- Follow all other specific instructions in the Litigation Hold.
- Consult with the designated contact person regarding any questions involving electronic records.

Litigation: Actual or "Reasonably Anticipated"

The obligation to preserve potential 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.

Factors to consider in deciding whether litigation is “reasonably foreseeable” or “reasonably likely” include:

- Historical Experience: Look at whether similar situations have led to litigation in the past.
- Filed Complaints: Be aware of complaints filed with the WSD or an enforcement agency, which may indicate a likelihood of future litigation.
- Significant Incidents: Pay attention to events resulting in known and significant injury.
- Attorney Statements: Examine any statements by an individual’s attorney regarding a dispute with the WSD.
- Employee Statements: Consider statements by WSD employees and officials regarding the potential of litigation.
- Initiation of Dispute Resolution Procedures: Give considerable weight to an action by a contractor to initiate a dispute resolution clause in a contract.
- Public Disclosure Requests: Consider whether a public disclosure request suggests the likelihood of future litigation. Although the WSD routinely receives public disclosure requests that are unrelated to litigation, some reasonably foreshadow a lawsuit.
- Event Reported In the Press: Take stock of particularly bad events that are reported in the press, where history suggests litigation is likely.
- 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.
- 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.

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 WSD’s normal retention schedules will apply to the documents. The Office of Risk Management and the

WSD's attorneys will be responsible for applying their own special retention schedules for "litigation" records.

Retrieval of Electronic Records for Discovery

In most cases, the need to actually produce preserved electronic records will come weeks or months after the preservation has occurred. When the WSD receives a request from an opposing party for production ("discovery") of electronic records, the WSD's counsel and primary WSD 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.
(See http://www.educause.edu/ir/library/pdf/EPO0664.pdf for a discussion of tradeoffs.)

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

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 in selecting the best approach to the specific request:

- 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.
- Enlisting WSD Technical Support: Sometimes the system administrator or other WSD technical support personnel will directly retrieve the responsive records due to particular concerns about an individual user's time, skill, or dependability in identifying the universe of responsive records. Such personnel are often able to bring to bear sophisticated tools for searching and extracting large volumes of responsive records.
- 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.

Factors to Consider in Records Retrieval

- Thoroughness: The approach in a specific case needs to be reasonably calculated to gather all potentially relevant records.
- Operational Efficiencies: The activities required should be operationally efficient to ensure timely preservation and processing of the data.
- Individual Privacy: The processes implemented to respond to electronic discovery must take into account personal privacy concerns.

- 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.
- Individual Disruption: Procedures should take into account potentially significant impacts in terms of time and effort for individuals named in the lawsuit.
- Procedural Consistency: The WSD will require that procedures developed to meet these new rules are consistently followed and executed.

Post-Retrieval Review

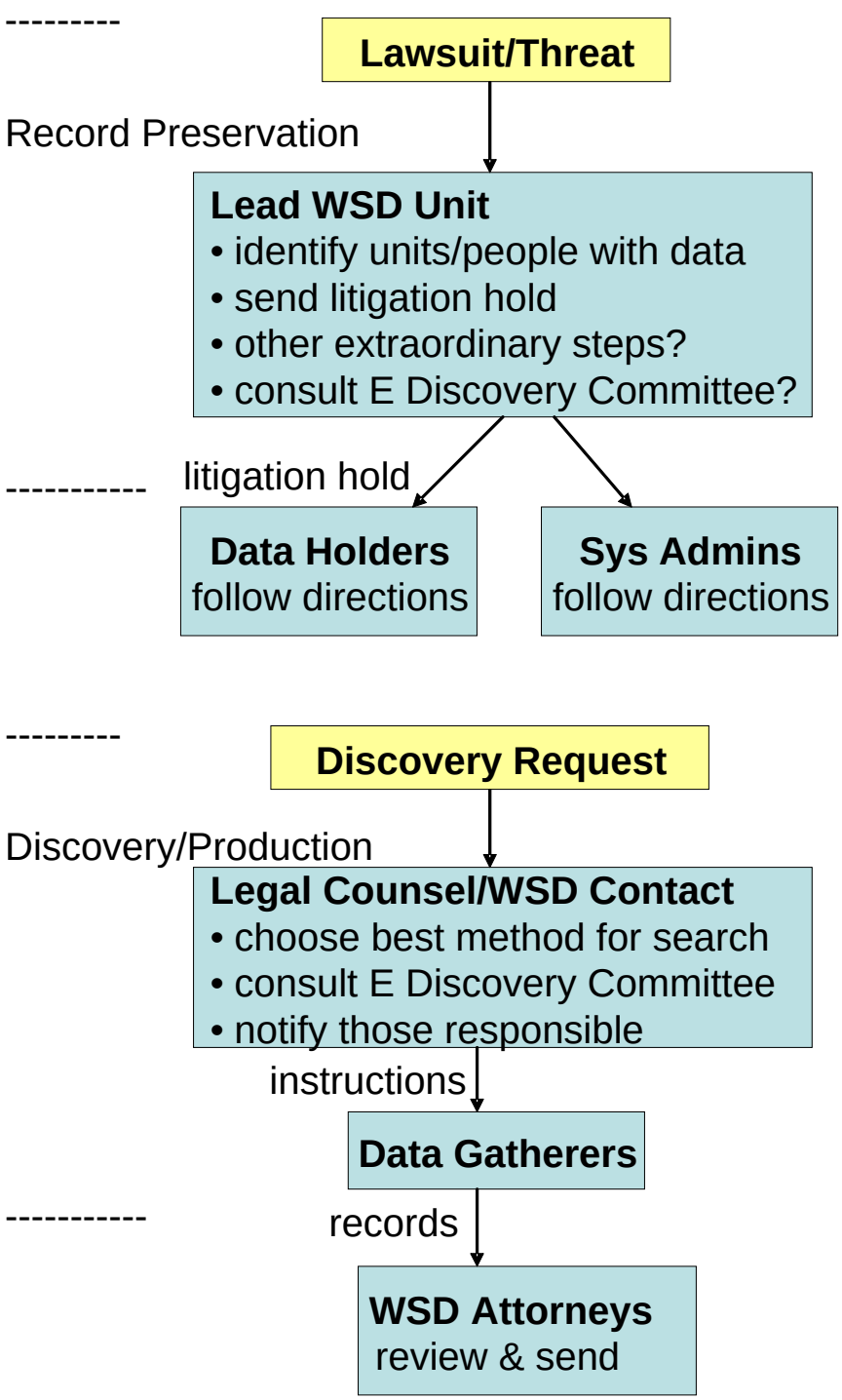
As potentially-responsive electronic records are gathered, the will be provided to the WSD attorneys for further processing.

Post-Production Duties

Preservation and production of information related to a lawsuit does not end with an initial production of records. Potentially relevant records generated after the Litigation Hold must be preserved for possible future retrieval.

Approved: July 25, 2008

ATTACHMENT 1 – FLOW CHART



ATTACHMENT 2 – FREQUENTLY ASKED QUESTIONS

1. What do "electronic discovery" and "data preservation" mean?

"Discovery" is the process by which potentially relevant documents are captured and produced by the parties in a lawsuit. One of the ways a party can obtain "discovery" of potentially relevant documents is by asking other individuals or entities to produce documents. Federal and state courts recognize that the term "documents" includes electronic data and that electronic data is subject to the same discovery rules as other documents potentially 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 WSD (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 WSD and all of its faculty and staff members are under a legal duty to preserve all documents, 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 potentially relevant to a lawsuit, wherever it is stored – at a WSD work station, on a laptop, or cellular phone, or at an employee's home. It includes all forms of electronic communications, e.g., e-mail, 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. However, back-up tapes may not have to be preserved, and the WSD should consult with their attorneys on a given case regarding the disaster recovery system procedures.

3. What will I have to do?

You will be notified of the responsibility to preserve electronically stored information (ESI) 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 WSD IT personnel in order to identify and preserve reasonably identifiable potential sources of 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 WSD's counsel and/or primary WSD contact (Risk Management, Human Resources or other unit) will advise you when you and the WSD 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 concluded. When preservation effort 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 should 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 WSD. Thus, if you use your home computer for WSD-related business (including e-mail on your WSD e-mail 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 be questioned under oath at a later date by an attorney representing the opposing party about what data you took off your computer. Thus, if you believe there is something personal on your computer, you should consult the Assistant Superintendent or Public Records Office before removing it. The material may also be a public record, and public records are subject to the WSD's retention policies.

7. **I previously deleted something that might be relevant – should I be concerned about that?**
Preservation of information arises when there is a lawsuit, reasonable anticipation of litigation, or if there has been a public records request. Electronically stored information deleted before a lawsuit, reasonable anticipation of a lawsuit or a records request that was properly deleted 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 WSD?**
You must also preserve any newly created documents 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 WSD staff members, applicable storage costs and the like) will be absorbed by the department.

10. **Who will be looking at WSD data from my computer?**
This depends on the reason for the Litigation Hold. If the matter involves a complaint or claim that requires investigation, appropriate WSD department 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 records in your computer files 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 WSD, 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 WSD'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?**
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 should I do with my electronic data if I leave the WSD?**
If you plan to leave your employment with the WSD during the pendency of a lawsuit for which you have received a preservation hold, you should confer with your supervisor, WSD IT staff and the Attorney General's Office or other contacts listed in the Litigation Hold notice.

14. **What if I have additional questions?**
Get in touch with the WSD's counsel and/or primary WSD contact (Risk Management, Human Resources or other unit) contacts listed in the Litigation Hold notice.

ATTACHMENT 3 – DOCUMENT PRESERVATION PLAN (SAMPLE)

Case or Matter: _____ Date: _____

Lead WSD Unit: _____

Primary Contact: _____
Name Phone Email

WSD Attorney (if any): _____
Name Phone Email

1. Units and Individuals Likely To Have Potentially-Relevant Documents

Operating Units	**Individuals**	**Send Lit Hold?/By?**

2. Are Additional Steps Needed?

Individuals	**Imagining?**	**Account Snapshot?**	**Hold Back-Ups?**	**System Checklist?**	**Other?**

3. Any Follow-Up Steps Needed?

☐ Reminders? _____

☐ Other? _____

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 WSD will 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 WSD Records Center and/or WSD 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
- e-mails
- 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 potentially relevant documents that can be reasonably identified 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 WSD 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 documents that can be reasonably identified as being potentially relevant

(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 since your receipt of this letter.

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

_____

_____

_____

ATTACHMENT 5 – ESI Locations

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 is not 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 all 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**

____ **Laptops**

____ **Desktops**

____ **PDAs**

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 WSD in responding to a potential or existing lawsuit.

Name _____
Date _____
Campus address _____
Campus phone _____
Email address _____

1. Computers
Please identify other computer systems (including home computers, laptops, blackberry, and personal digital assistants) you use to conduct WSD 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 WSD, you do not need to list it.

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

2. Data storage
Besides the internal hard disc(s) in the above systems(s), please list the other places where you store electronic data related to your position at the WSD. Note that back-ups 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 $** WSD $ 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 WSD-related messages. If you store messages on a local computer, give the associated system number(s).

Service WSD 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 WSD 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 provides your computing and networking support.

Name _____
Email address _____
Phone number _____
Employee Signature _____

ATTACHMENT 7 – STATEMENT OF COMPLIANCE

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

I was assigned responsibility by the Washington School for the Deaf 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 WSD's legal team, I conducted a reasonable, diligent and good faith search of the files and records in my possession or control.

To the best of my knowledge, information and belief, I have identified the potentially relevant documents maintained in the ordinary course of business that may be responsive to the requests for production have been provided to the representative of the WSD's legal team. I am aware of no documents in WSD 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

_____
Washington School for the Deaf

_____

_____

_____
Files For Which I Was Assigned Search Responsibility

Others Who Assisted:

_____

_____

_____

_____

_____