Evidence Preservation & Electronic Discovery
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. Upon notice that a lawsuit has been commenced against CCS (or a charge filed with an administrative agency) or if it is reasonably anticipated that a lawsuit may be brought (or a charge filed), CCS 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 CCS 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 (e.g., metadata), is also available for inspection. In other words, it is not sufficient to make a hard copy of electronic records. However, back-up media may not have to be preserved, and CCS will consult with the Attorney General's Office (AGO) 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." The CCS Chief Financial Officer (CFO) is the designated Risk Manager and will issue the hold notice. You will then be asked to cooperate with the Attorney General's Office, the Office of Risk Management, and/or CCS 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 AGO and/or CFO, through the CCS point of contact, will advise you when you and CCS 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 state records retention 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 also need to preserve data on my home computer?

Yes, if you use it for work. The same rules apply to any computer that stores information potentially relevant to a lawsuit involving CCS. Thus, if you use your home computer for CCS-related business (including e-mail on your CCS 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 CFO or AGO before removing it. The material may also be a public record, and public records are subject to state records 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 CCS?
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 pays 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 CCS staff members, applicable storage costs and the like) will be absorbed by the department.

10. Who will be looking at CCS 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 CCS department personnel from departments such as the Office of Risk Management, Human Resources, 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?
CCS, 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 AGO 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 if I don't want to disclose my CCS data?
CCS and its employees have a legal duty to preserve and, subject to the rules governing discovery, turn over its records, including 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 CCS and/or you individually and adversely impact findings in the litigation. CCS will take steps to protect your privacy and to ensure that protected or 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 records and electronic data if I leave CCS?
If you plan to leave your employment with CCS during the pendency of a lawsuit for which you have received a litigation hold, you should confer with the CCS point of contact listed in the Litigation Hold Notice.

15. What if I have additional questions?
Get in touch with the CCS point of contact listed in the Ligation Hold Notice.

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

Systems administrators and computer users at CCS 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	Objective	Features
Disaster Recovery	To serve as a "safety net" to enable immediate restoration of file structure and content in case of a system "crash"	➢ 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	Some or all of the following: ➢ 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	➢ 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**

Evidence Preservation & Electronic Discovery
Making Secure Preservation Copies

CCS Technology and other system administrators at CCS 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 CCS 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 unreasonable burdens on CCS (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) CCS and the individual user agree that making a secure preservation copy would be convenient.

a. Risk to Integrity of Records

CCS 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:

i. The account or computer is known to contain records with an exceptional value to CCS.
ii. The form or location of the records makes them unusually volatile.
iii. The records are subject to the operation of an automated system that may otherwise dispose of them.
iv. 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 CCS and a specific user will wish to make a secure preservation copy of records:

i. In order to facilitate a search for records; or
ii. 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 of these purposes after discussion with the user. In considering making such a copy for the mutual convenience of the user and CCS, 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?

CCS 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.

6$03/(/,7,*$7,21 +2/'127,&(

Subject: Litigation Hold Notice
Attachments: Evidence Checklist.pdf

Importance: High

Dear Colleagues. Attached is a copy of a _____ filed by _____. The filing of this claim creates an obligation on CCS and its employees to preserve and hold all documents and emails that may reasonably be considered relevant to the claim. You are receiving this notice because you may have records relevant to this claim and you must take reasonable and prompt steps to identify and preserve those records. In addition, if you are aware of other documents that may be relevant but which you do not currently have access to, please let me know. This Notice also applies to duplicate records. Courts can impose serious penalties for failure to preserve and provide relevant information.

"Document" is defined in the court rules as including "writings, emails, drawings, graphics, charts, photographs, phone records, images, and other data compilations from which information can be obtained[.]" CR 34. This definition includes traditional paper documents, but it also includes a wide range of additional items such as calendars, diaries, Post-It® notes, and draft documents. It includes electronically stored information in all forms, including Word and other word processing files, Excel and other spreadsheet files, Access and other data base files, and electronic files of all forms stored on personal computers, laptops, tablets, network servers, backup media, cell and smart phones, and all kinds of removable electronic media storage (CDs, DVDs, floppy disks, USB drives, etc.). It includes existing documents and documents created in the future.

To ensure that we retain all relevant records, we ask that you search all records in your possession or control that could reasonably relate to this claim, and take prompt action to preserve that information. If questions exist about the relevance of a document, you should err on the side of preserving the document. Under no circumstances should you delete, destroy or damage any existing related records, including e-mail. Electronic records such as e-mail should be preserved by creating electronic folders, or other media storage, and transferring all related e-mails to those folders or media. You should not delete, destroy or automatically remove any electronic records that might reasonably relate to this claim. **This Notice supersedes all retention destruction schedules; <u>all such schedules must be suspended</u> as to records covered by this Notice.** You will be notified by this office if you need to provide these records and/or when the Hold Notice is lifted.

Attached is a Potential Evidence Checklist/Verification form. Please use this form to document the types of records you have related to this claim. Return the completed and signed form to _____ at MS _____ by close of business on _____.

If you have questions or need help to identify and preserve records, please contact _____.

Community Colleges of Spokane

Potential Evidence Checklist/Verification

I was assigned the responsibility by CCS to search for all records and other potential evidence that may be pertinent to [**INSERT CASE NAME**].

In accordance with the instructions, procedures, and directions received in the Litigation Hold Notice dated _____, I have conducted a reasonable, diligent, and good faith search of the files and records in my possession or control. I have searched all materials that I have access to at work or elsewhere, including paper and electronically stored information.

To the best of my knowledge, information, and belief, I have identified the potentially relevant records maintained in the ordinary course of business that may be responsive to this legal matter. I am aware of no documents in the CCS files that are responsive that have not been thus provided, and I have no reason to believe that any such documents exists.

Based on my review, I have the following media containing information that is or could be relevant to this claim.

Official File Material:	☐ Yes ☐ No	Notes:	☐ Yes ☐ No
Drafts:	☐ Yes ☐ No	Server File Material:	☐ Yes ☐ No
Computer File Material:	☐ Yes ☐ No	File Hosting or Cloud Storage	☐ Yes ☐ No
Remote Hard Drives	☐ Yes ☐ No	USB Storage Devices:	☐ Yes ☐ No
Flash or Zip Drive Disks:	☐ Yes ☐ No	Other Storage Media:	☐ Yes ☐ No
Computer CD/DVD Disks:	☐ Yes ☐ No	Privately Owned Devices:	☐ Yes ☐ No
Agency Specialty Software:	☐ Yes ☐ No	E-mail:	☐ Yes ☐ No
Audio or Video Recordings:	☐ Yes ☐ No	Other Recordings:	☐ Yes ☐ No
Drawings or Photographs:	☐ Yes ☐ No	Any Other Material:	☐ Yes ☐ No
Non-Official File Material:	☐ Yes ☐ No		

Comments/Notes: _____

_____

_____

Signature: _____

_____ _____

Printed Name Printed Date

Please return this completed document by close of business _____, to _____

If you have questions contact _____. Thank you for your assistance.

Community Colleges of Spokane

Computer System Checklist – Individual

This checklist is provided to help you determine and document potential locations of electronically stored information (ESI) that may be relevant to [**INSERT CASE NAME**]. Once you have completed this checklist, please return it to [**INSERT POINT OF CONTACT & MS**].

Date: _____ **Name:** _____

Email: _____ **Phone:** _____ **Mail Stop:** _____

1. Computers

Please identify all computer systems (including home computers, laptops, cell/smart phones, and personal digital assistants) you use to conduct CCS 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 CCS, you do not need to list it.

No.	Name	Type Desktop, Laptop, PDA, Tablet, etc.	Ownership District 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 CCS. 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, USB Storage Device, File Hosting or Cloud Storage?	Purchase $ District $ or Personal $?	Location of Use Home, office, travel, all?	Computer Number

3. Backups

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

Computer Number	**Type and Location** CCS Network Backup, Local Storage Media, File Hosting, or Cloud Storage, etc.?	**Schedule for Backup** Daily, weekly, irregularly?

4. Email Service Provider

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

Service CCS Email System, Personal Email Service Provider (Comcast, MSN, Gmail, Yahoo, etc.)	**Use** Work, personal, or both?	**Messages Stored Locally?** on Computer Number.

5. Collaborative work

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

Collaborative System Wiki, SharePoint, Web Page,	**Location** URL, archives, etc.	**Purpose of System**?

To the best of my knowledge, information, and belief, I have identified all the potentially relevant computer systems that I use in the ordinary course of business that may be responsive to this case.

Signature: _____

_____ _____

Printed Name Printed Date

Community Colleges of Spokane

Computer System Checklist – Administrator

This checklist may be of use to systems administrators as they determine potential locations of electronically stored information (ESI) that might assist CCS 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 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 Storage 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.

____ **Portable Storage Media** (Media Cards, CD/DVD, Flash Drives, etc.).

____ **Computers** (Desktops, Laptops, Tablets, Ultra-Mobile PCs, etc.).

____ **Portable Electronic Devices (Cellphones, Smartphones, PDA, IPads, IPods, etc.).**

Notes: Please provide any additional information you think would be helpful in understanding CCS's Electronically Stored Information file types and locations that may be responsive to this matter.

Community Colleges of Spokane

Information Preservation Plan

Case or Matter: _____ **Assigned AAG (if any):** _____ **Date:** _____

Primary Unit: _____ **Lead Contact:** _____ **Litigation Hold Sent (Date):** _____

LITIGATION HOLD CONTACT INFORMATION – INDIVIDUALS LIKELY TO HAVE POTENTIALLY RELEVANT RECORDS:

Name	Phone	Email	Mail Stop	Compliance Checklist Rcv'd (Date)	Has Records (Yes/No)	Other Notes

ARE ADDITIONAL STEPS NEEDED?

Individuals	Imaging?	Account Snapshot?	Hold Back Ups?	System Checklist?	Other?