Implementing Board Policy 1.50.02
Contact: Chief Financial Officer, 434-5275

1.0 Purpose

Court decisions and rules place obligation on public and private organizations to preserve all reasonably identifiable potential evidence in all forms when litigation has been filed or is reasonably anticipated or reasonably foreseeable. Failure to take reasonable steps to preserve records and other evidence could lead to significant sanctions by the courts. This procedure provides evidence preservation guidance and protocols applicable in the event of litigation or potential litigation to which CCS is a party.

2.0 Limitations and Requirements

- 2.1 This procedure applies to all documents and other potential evidence owned or under the control of CCS or its employees. It requires preservation of potential evidence, including but not limited to electronically stored information (ESI) in its original (native) format, regardless of format or medium, when litigation is reasonably anticipated or is reasonably foreseeable.
- 2.2 The CCS Records Officer manages and oversees CCS compliance with state and federal laws and regulations relating to the preservation and destruction of electronic and paper information. The Chief Financial Officer is the designated CCS Records Officer.
- 2.3 In absence of reasonably anticipated litigation, CCS public records are preserved, retained, or disposed in a manner consistent with 1.50.02-B Records Management and relevant state and federal law. When a lawsuit is filed or reasonably anticipated employees are obligated to immediately suspend destruction or disposal of records, tangible items and other potential evidence in the litigation. This procedure supersedes any provision in 1.50.02-B or other CCS, unit, or department practice that would otherwise authorize destruction or disposal of such potential evidence.

3.0 Definitions

The following definitions are specific to the terms of this procedure and do not modify or revise similar terms as used in related procedures.

- 3.1 <u>Cabinet</u>: CCS Executives, including the Chancellor, College Presidents and Vice Presidents, Chief Administration Office, Chief Financial Officer, Chief Information Officer, Provost/Chief Learning Officer, and the Public Information Officer.
- 3.2 <u>Unit</u>: Spokane Community College (SCC), Spokane Falls Community College (SFCC), or District Administration (District)
- 3.3 Risk Manager: The Chief Financial Officer is the designated CCS Risk Manager.
- 3.4 <u>Point of Contact</u>: The CCS representative designated to assist the Attorney General's Office and coordinate contact with CCS employees regarding the legal issue, as necessary.
- 3.5 <u>Information Preservation Team</u>: CCS's assigned Assistant Attorney General, the Chief Financial Officer, Chief Information Officer, Chief Administration Officer, or designees who coordinate evidence preservation efforts in response to complex litigation or potentially complex reasonably anticipated litigation to which CCS is a party. Unit-specific personnel may be added on an ad hoc basis as appropriate to each legal issue.

- 3.6 <u>Electronically Stored Information (ESI)</u>: Computer data or electronic recorded media of any kind that is stored in an electronic form that can be retrieved and examined. Examples of ESI include, but are not limited to: email messages, word-processing documents, spreadsheets, databases, digital images, video and audio files, web pages, instant messages, blogs, calendars, Internet cookies, Internet bookmarks and/or favorite addresses. ESI may be located on network servers, backup tapes, cloud storage, PDAs, flash drives, CDs, DVDs, floppy disks, work computers, telephone systems, cellular telephones, laptops, tablets, or any other device used to do CCS work. Such evidence may also be located on any personal or privately-owned devices used at an individual's home or otherwise for such purpose.
- 3.7 <u>Potential Evidence</u>: Any record, document or tangible item that may reasonably be expected to be requested in discovery, used in, or related to litigation to which CCS is or may reasonably be a party. Nothing in this procedure precludes or alters duties to preserve physical evidence such as models, damaged equipment, and other tangible items.
- 3.8 Record: Any document or recorded information regardless of physical form or characteristics created, sent, organized, received, or otherwise possessed by CCS in the course of public business. Records may include, but are not limited to, paper documents drawings, graphs, charts, videotapes, digital images (still or moving), recordings, photographs, telephone records, data compilations, planners, calendars, diaries, and draft documents.
- 3.9 <u>Tangible Evidence</u>: Physical or tangible evidence may include a wide variety of items. Examples include, but are not limited to, hard copies of records or documents, physical evidence relative to an accident (i.e., debris, damaged equipment or vehicles), statements, and test results. The kind of physical evidence that exists depends on the situation.

4.0 Litigation – Actual or Anticipated

- 4.1 When litigation has been filed, the Risk Manager determines which units and/or individuals may hold potential evidence. The Risk Manager issues a Litigation Hold Notice and proceeds in accordance with this procedure, unless a Litigation Hold Notice has been or will be imminently issued by another entity (e.g., the Office of Attorney General). If another entity issues the Notice, CCS cooperates with the obligations of that Notice.
- 4.2 When the Risk Manager receives information from CCS employees or other sources that litigation is reasonably anticipated or foreseeable, the Risk Manager consults with the Office of the Attorney General (who provides legal advice) to determine whether a litigation hold notice should be issued. If appropriate, the Risk Manager issues a litigation hold notice and proceeds in accordance with this procedure.
- 4.3 A determination of whether litigation is reasonably anticipated or foreseeable is made based on the specific facts and circumstances at issue. Factors to consider in deciding whether litigation is "reasonably foreseeable" or "reasonably likely" may include, among other things:
 - 4.3.1 Historical Experience: Similar situations that in the past led to litigation.
 - 4.3.2 Filed Complaints: Complaints filed with CCS or an enforcement agency.
 - 4.3.3 Significant Incidents: Events resulting in known or significant injury, especially if it is an unusual event.
 - 4.3.4 Attorney Statements: Statements by an attorney regarding a dispute with CCS.
 - 4.3.5 Employee Statements: Statements by employees or officials regarding potential litigation.

- 4.3.6 Initiation of Dispute Resolution Procedures: Initiation of a dispute resolution clause in a contract.
- 4.3.7 Public Disclosure Requests: Public disclosure requests which suggest likely future litigation
- 4.3.8 Event Reported in the Press: Events reported in the press where history suggests litigation is likely.

5.0 Information Preservation Team and Preservation Plan

- 5.1 The Risk Manager convenes the Information Preservation Team when team expertise is needed due to potentially complicated or voluminous preservation of potential evidence. The Information Preservation Team works in conjunction with the designated point of contact to gather and preserve relevant information consistent with applicable laws and CCS policies.
- In such cases, the Information Preservation Team may decide to develop a written preservation plan outlining immediate steps that need to be taken, including:
 - 5.2.1 Identifying the departments, units, and individuals who might possess potentially relevant information.
 - 5.2.2 Coordinating preservation and production advice and practices.
 - 5.2.3 Gathering a summary of the hardware and software involved.
 - 5.2.4 Determining whether more aggressive steps (such as "imaging" or sequestering computers, securing and removing storage media from scheduled rotation, or taking snapshots of network folders) are warranted.
 - 5.2.5 Establishing a method for following up, which may include sending out reminders, conducting preservation compliance checks, and addressing new questions or issues from employees with potential evidence.
- 5.3 Circumstances that may favor development of a written preservation plan include litigation or reasonably anticipated or foreseeable litigation:
 - 5.3.1 That may involve a large quantity of CCS records or other potential evidence;
 - 5.3.2 In which control over potential evidence resides in multiple locations throughout CCS;
 - 5.3.3 That focuses on CCS management of records such as public records litigation; and/or
 - 5.3.4 In which there is significant risk that potential evidence may be destroyed or disposed absent additional measures.

6.0 What Must Be Preserved

- 6.1 All reasonably identifiable potential evidence must be preserved when litigation to which CCS is a party has been filed or is reasonably anticipated or foreseeable. When in doubt, employees should err on the side of preserving potential evidence.
- All evidence is to be preserved in as close to its original form as possible. Tangible evidence may not be altered or destroyed when litigation is pending or reasonably anticipated, except with the express written permission of the Risk Manager in consultation with the Office of the Attorney General. ESI must be preserved in its original (native) form.

7.0 Litigation Hold Notice

- 7.1 A Litigation Hold Notice is formal notification that litigation to which CCS is a party has been filed or is reasonably anticipated or foreseeable. It gives notice that potential evidence which CCS must preserve may be in the recipient's possession or scope of responsibility and that the recipient, as an employee of CCS, must immediately take reasonable steps to preserve such information. In particular, the recipient must:
 - 7.1.1 Suspend any CCS or departmental policies or procedures that might call for the routine destruction of records constituting potential evidence under the recipient's control. The Litigation Hold supersedes all document retention and destruction schedules.
 - 7.1.2 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 be suspended.
 - 7.1.3 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.
 - 7.1.4 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.
 - 7.1.5 Protect and preserve all relevant documents including any hard copies of electronic records.
 - 7.1.6 Protect and preserve any new documents that are generated or received that may be relevant to the litigation after receipt of a Litigation Hold.
 - 7.1.7 Advise the Risk Manager, Point of Contact, or Information Preservation Team of any personal information that may potentially be affected by the Litigation Hold.
 - 7.1.8 Follow all other specific instructions in the Litigation Hold.
 - 7.1.9 Consult with the Risk Manager, Point of Contact, or Information Preservation Team regarding any questions involving potential evidence.
- 7.2 A Potential Evidence Checklist/Verification form is routed with each Litigation Hold Notice. The Notice requires the recipient to confirm receipt by returning the checklist indicating that the recipient has:
 - 7.2.1 Responsive information, identified its forms, and taken steps to preserve the information.
 - 7.2.2 No information responsive to the Litigation Hold Notice.

8.0 Retrieval of Electronic Records for Discovery

8.1 In most cases, the need to actually produce preserved records or evidence will come weeks or months after the preservation has occurred. The Attorney General's office will notify CCS of requests from an opposing party for production ("discovery") of records. The CCS designated point of contact for the legal issue, in conjunction with the Information Preservation Team, will determine the best approach to take in order to efficiently produce a complete and accurate response.

- 8.2 The response may consist of any or all of the following:
 - 8.2.1 supplying the requested information;
 - 8.2.2 attempting to obtain a modification of the request (e.g., by narrowing the request's scope or obtaining agreement as to specific search terms);
 - 8.2.3 declining to provide some or all of the requested data based upon expense of production or other basis.
- 8.3 Where some or all of the requested electronic records must be retrieved, reviewed, and potentially disclosed, the following options will be considered in selecting the best approach to the specific request:
 - 8.3.1 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.
 - 8.3.2 Enlisting CCS Technical Support: Sometimes the system administrator or other CCS 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,
 - 8.3.3 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.
- 8.4 Factors that will be considered in records retrieval include:
 - 8.4.1 Thoroughness: The approach in a specific case will be reasonably calculated to gather all potentially relevant records.
 - 8.4.2 Operational Efficiencies: The activities will be operationally efficient to ensure timely preservation and processing of the data.
 - 8.4.3 Individual Privacy: The processes implemented to respond to electronic discovery will take into account personal privacy concerns.
 - 8.4.4 Risk of Data Loss: Reasonable steps will be taken to protect data from loss through inadvertent or intentional deletion of files or loss of data storage media.
 - 8.4.5 Individual Disruption: Procedures will take into account potentially significant impacts in terms of time and effort for individuals named in the lawsuit.
 - 8.4.6 Procedural Consistency: CCS will ensure that this procedure is consistently followed and executed.

9.0 Post-Retrieval Review and Responsibilities

- 9.1 As potentially responsive records are gathered, they will be held by the owner until they are contacted by the CCS point of contact or the Attorney General's Office for further processing.
- 9.2 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.

- 9.3 When the litigation or threat of litigation that prompted the Litigation Hold has ended, the Risk Manager informs those who received the notice that they are no longer under any special obligations to preserve the identified categories of materials. At that point, CCS's normal document retention schedules will apply to the documents.
- 9.4 The CCS Risk Manager and Attorney General's Office will be responsible for applying their own special retention schedules for "litigation" records.

10.0 Related Information

- 10.1 RCW 40.14 Preservation and Destruction of Public Records
- 10.2 RCW 40.14.040 Records Officers Designation Powers and Duties
- 10.3 CCS Administrative Procedure 1.50.02-B Records Management
- 10.4 Evidence Preservation Process Flow Chart
- 10.5 Evidence Preservation & Electronic Discovery, Related Material
 - Frequently Asked Questions
 - Making Secure Preservation Copies
 - Litigation Hold Notice
 - Potential Evidence Checklist/Verification
 - Computer System Checklist Individual
 - Computer System Checklist Administrator
 - ➤ Information Preservation Plan

Originated: October 2013

Cabinet approval: October 28, 2013

