BBCC ADMINISTRATIVE PROCESS

<table>
<thead>
<tr>
<th>TITLE: Records Management</th>
<th>PAGE: 1 OF 1</th>
<th>NUMBER: 8060</th>
<th>REVIEWED: REVISED: NEW</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORIGINATING DEPARTMENT: Purchasing</td>
<td>EFFECTIVE DATE: 10/14/14</td>
<td>SUPERSEDES NO. DATE:</td>
<td></td>
</tr>
<tr>
<td>DATE CABINET APPROVAL: 10/13/14</td>
<td>APPROVED BY:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

President

Objectives:

Big Bend Community College (BBCC) recognizes the need for orderly management and retrieval of all official public records and a documented records retention and destruction schedule. The purpose of this program is to establish standardized procedures according to the provision of Public Records Act (RCW 40.14) and all other state and federal statutes and regulations which govern records keeping practices. These practices include the systematic identification and disposal of obsolete records for the minimum periods stated in the Washington General Records Retention Schedules, which are located at http://www.secstate.wa.gov/archives; transfer of historically valuable records to the Division of Archives; removal of non-current or inactive records from active office storage; protection and security of records essential to the college's authority and operation; disaster preparedness; insurance of records systems integrity and accessibility; and effective compliance with public disclosure requirements.

Location:

BBCC's records storage is located in the basement of Building 1500.

Responsibility:

College offices and departments are responsible for securely maintaining records for the designated retention period indicated on the retention schedule. The department's responsibility includes ensuring the physical safety of the records, as well as ensuring that confidential records are protected from inappropriate or illegal access and/or release.

College records are public records and may be destroyed, microfilmed, or permanently removed only in accordance with establish guidelines. No employee has, by virtue of his/her position, any personal or property right to public records even though she/he
may have helped develop or simplify them. The unauthorized destruction, removal, or use of college records is a violation of RCW 40.15 and a criminal offense.

**Retention and Disposition of Records:**

A Control Card is to be used to track the process of initiating records storage, records sent to archives, and records tagged for disposal and a database maintained of the information collected from the Control Cards. **The Control Card template is located on the Big Bend portal under New Record Retention link.**

The Records Coordinator(s) will initiate removal of records to storage, archives, or the disposal of non-active office records in accordance with the **General Records Retention Schedule and Records Management Manual** and consistent with the college process set forth herein.

- **Non-active records to storage:**
  The Records Coordinator will place the non-active records in an approved archive box, provide the necessary information on the Control Card and secure it to the outside of the box, forward a copy of the Control Card to the Records Retention Officer, and email the Central Receiver to place the records in storage.

- **Transfer records to archives:**
  The Records Retention Officer must review the historical records to transfer to the regional branch of the Division of Archives.

- **Records to be destroyed:**
  Upon verification by the RRO that the records retention period has been satisfied, records may be destroyed by an appropriate method (shredding by the state-approved company).

**Electronic Records**

Electronic records must be retained in electronic format and remain useable, searchable, retrievable and authentic for the length of the designated retention period. Electronic records, including email, must be retained and disposed of based on their content. Electronic records are retained under the same retention schedule as paper records with identical content.

- **Categories of email messages which are likely to be public records:**
  1. Policy and procedure directives.
  2. Correspondence or memoranda related to official business.
  3. Agendas and minutes of meetings.
  4. Documents related to legal or audit issues.
  5. Messages which document agency actions, decisions, operations, and responsibilities.
  6. Documents that initiate, authorize, or complete a business transaction.
  7. Drafts of documents that are circulated for comment or approval.
  8. Final reports or recommendations.
9. Email calendars reflecting the daily appointments of officials conducting state business.
10. Email distribution lists for state business electronic mail.
11. Information downloaded from network sources such as the World Wide Web may be a public record if it is used in support of the functions listed above.

- Non-public records that can be deleted: (Delete these as soon as possible)
  1. FYI or information requiring no action.
  2. Social meeting or announcements.
  3. Personal messages and chit chat.
  4. Spam and junk mail.
- Other types of electronic messaging
  1. Database.
  2. Text Messaging.
  3. Instant Messaging.
  4. Voice Mail.
  5. Social Media.
- Filing electronic records
  1. Do an inventory.
  2. Create files just like paper files

As public employees, everyone has a legal responsibility for the public records they create and use.

EVIDENCE PRESERVATION FOR LITIGATION HOLDS

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 BBCC 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 BBCC 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 Records Officer manages and oversees BBCC’s compliance with state and federal laws and regulations relating to the preservation and destruction of electronic and paper information.

2.3 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 other BBCC, unit, or department practice that would otherwise authorize destruction or disposal of such potential evidence.

3.0 Litigation – Actual or Anticipated

3.1 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, BBCC cooperates with the obligations of that Notice.

3.2 When the Risk Manager receives information from BBCC 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.

3.3 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:

3.3.1 Historical Experience: Similar situations that in the past led to litigation.

3.3.2 Filed Complaints: Complaints filed with BBCC or an enforcement agency.

3.3.3 Significant Incidents: Events resulting in known or significant injury, especially if it is an unusual event.

3.3.4 Attorney Statements: Statements by an attorney regarding a dispute with BBCC.
3.3.5 Employee Statements: Statements by employees or officials regarding potential litigation.

3.3.6 Initiation of Dispute Resolution Procedures: Initiation of a dispute resolution clause in a contract.

3.3.7 Public Disclosure Requests: Public disclosure requests which suggest likely future litigation.

3.3.8 Event Reported in the Press: Events reported in the press where history suggests litigation is likely.

4.0 Litigation Hold Notice

4.1 A Litigation Hold Notice is formal notification that litigation to which BBCC is a party has been filed or is reasonably anticipated or foreseeable. It gives notice that potential evidence which BBCC must preserve may be in the recipient’s possession or scope of responsibility and that the recipient, as an employee of BBCC, must immediately take reasonable steps to preserve such information. In particular, the recipient must:

4.1.1 Suspend any BBCC 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.

4.1.2 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.

4.1.3 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.

4.1.4 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.

4.1.5 Protect and preserve all relevant documents including any hard copies of electronic records.
4.1.6 Protect and preserve any new documents that are generated or received that may be relevant to the litigation after receipt of a Litigation Hold.

4.1.7 Advise the Risk Manager and/or Point of Contact of any personal information that may potentially be affected by the Litigation Hold.

4.1.8 Follow all other specific instructions in the Litigation Hold.

4.1.9 Consult with the Risk Manager and/or Point of Contact regarding any questions involving potential evidence.

4.2 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:

4.2.1 Responsive information, identified its forms, and taken steps to preserve the information.

4.2.2 No information responsive to the Litigation Hold Notice.

5.0 What Must Be Preserved

5.1 All reasonably identifiable potential evidence must be preserved when litigation to which BBCC 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.

5.2 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.

6.0 Retrieval of Electronic Records for Discovery

6.1 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 BBCC of requests from an opposing party for production ("discovery") of records. The BBCC designated point of contact for the legal issue will determine the best approach to take in order to efficiently produce a complete and accurate response.

6.2 The response may consist of any or all of the following:
6.2.1 supplying the requested information;

6.2.2 attempting to obtain a modification of the request (e.g., by narrowing the request's scope or obtaining agreement as to specific search terms);

6.2.3 declining to provide some or all of the requested data based upon expense of production or other basis.

6.3 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:

6.3.1 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.

6.3.2 Enlisting BBCC Technical Support: Sometimes the system administrator or other BBCC 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.

6.3.3 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.

6.4 Factors that will be considered in records retrieval include:

6.4.1 Thoroughness: The approach in a specific case will be reasonably calculated to gather all potentially relevant records.

6.4.2 Operational Efficiencies: The activities will be operationally efficient to ensure timely preservation and processing of the data.

6.4.3 Individual Privacy: The processes implemented to respond to electronic discovery will take into account personal privacy concerns.
6.4.4 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.

6.4.5 Individual Disruption: Procedures will take into account potentially significant impacts in terms of time and effort for individuals named in the lawsuit.

6.4.6 Procedural Consistency: BBCC will ensure that this procedure is consistently followed and executed.

7.0 Post-Retrieval Review and Responsibilities

7.1 As potentially responsive records are gathered, they will be held by the owner until they are contacted by the BBCC point of contact or the Attorney General’s Office for further processing.

7.2 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.

7.3 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, BBCC’s normal document retention schedules will apply to the documents.

7.4 The BBCC Risk Manager and Attorney General’s Office will be responsible for applying their own special retention schedules for “litigation” records.

8.0 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.

8.1 Active Files – Active files are those files needed to support the current college business activity of a department or office. The active period may be determined by the records category.

8.2 Archival Files – Archival files are those files which have long-term value to the college, such as historical documents.

8.3 Confidential
Records – Confidential records include records which are exempt from public disclosure. Examples of confidential records include student files.

8.4 Electronic Mail – Electronic mail or email is meant to encompass all forms of electronic messaging such as instant messaging and all other current and emerging communication technologies. Work-related emails are public records and must be treated as such.

8.5 Electronically Stored Information (ESI): 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 BBCC 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.

8.6 Inactive Files – Inactive files are those for which the active period has passed and are being held for the remainder of the specified retention period. Inactive files may be relocated to building 1500. Each inactive file must be labeled with content description and disposition date. The new record retention label is located on the portal.

8.7 Point of Contact: The BBCC representative designated to assist the Attorney General’s Office and coordinate contact with BBCC employees regarding the legal issue, as necessary.

8.8 Potential Evidence: Any record, document or tangible item that may reasonably be expected to be requested in discovery, used in, or related to litigation to which BBCC 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.

8.9 Public Records – The term “public records” shall include any paper, correspondence, completed form, bound record book, photograph, film sound recording, map drawing, machine-readable material, electronic mail or messages or other documents, regardless of form or physical characteristics, that has been created or received by BBCC during the course of public business (RCW 40.14.010).

8.10 Record: Any document or recorded information regardless of physical form or characteristics created, sent, organized, received, or otherwise
possessed by BBCC 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.

8.11 Records Coordinators – Each department or office has a designated Records Retention Coordinator. This employee coordinates the preparation of the Records Retention Schedule, reviews the schedule biennially, and supervises retention and disposition of office records.

8.12 Records Management – A systematic control of information from creation to final disposition. A records management program contains three basic goals: 1) to fulfill legal mandates and responsibilities; 2) to store records in the most efficient and cost-effective manner possible; and 3) to assure access, protection, and security to the documentary history of governments (RCW 40.14.010).

8.13 Records Retention Office (RRO) – Each college designates a Records Retention Officer. The RRO has a fundamental responsibility to develop a comprehensive records management program. The RRO represents the college in all contact with the Records Officer of the SBCTC.

8.14 Risk Manager: The Vice President of Financial and Administrative Services is the designated BBCC Risk Manager.

8.15 Tangible Evidence: 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.

8.16 Web Storage – This is a new procedure that deals with storing of public records on the Internet. When transferring public records from paper to another format that can be stored on the internet, it must be approved by Washington State Archives, Office of the Secretary of State. The RRO has the form known as DAD, Destruction After Digitization. DAD is early destruction of non-archival paper records that have been digitized. Archival paper records may be digitized but never destroyed.

9.0 Related Information

RCW 40.14 Preservation and Destruction of Public Records
RCW 40.14.040 Records Officers – Designation – Powers and Duties

Evidence Preservation Process Flow Chart

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