


7 - INFORMATION SYSTEMS and SERVICES

700..... Acceptable Use of Information Systems and Services

705..... E-mail Retention Policy

720..... Accessible Technology Policy

725..... eSignatures and Submissions

	Chapter 7 – Information Systems and Services
Administrative Policy	ACCEPTABLE USE OF INFORMATION SYSTEMS AND SERVICES POLICY 700

700 Information Systems and Services: Employee Acceptable Use

Lower Columbia College Information Systems and Services include, but are not limited to, all local and wide area networks, Internet access, electronic publishing systems, www.lowercolumbia.edu, e-mail systems, administrative data processing systems, desktop computers, student labs, telephone systems, video systems, and all other current or future information systems.

The purpose of this policy is to protect the integrity and usability of College information systems and services and to insure their continued availability for student learning and conduct of college business. This policy applies to all College employees who are users of any of the College’s information systems or services.

Users of any of the College’s information systems or services agree to comply with applicable state, federal, and local laws, WAC code, and college policies and procedures.


- **Adopted 2/08**

Resources, References, Procedures, or contact information relating to this policy

Resource/Reference/Procedure	Title	Unit Responsibility
Procedure 700.1A	<u>Information System and Services – Employee Acceptable Use Policy</u>	VP Administration/Director of Information Services
<u>RCW 42.52.160(3)</u>	Ethics in Public Service	

Historic Review:

- Reviewed by the Cabinet and Leadership Team November 2008
- Campus Review: February 1-22, 2009
- Approved 2/23/09

	Chapter 7 – Information Systems and Services
Administrative Policy	E-MAIL RETENTION POLICY POLICY 705

705 E-Mail Retention

This policy is intended to help employees and students of Lower Columbia College determine what information sent or received by email should be retained and for how long, and is meant to address typical records that may be contained in email and does not necessarily reference other types of records, such as paper or other types of electronic files or data. Those records are covered in depth by the State Board for Community and Technical College record retention policy.

The policy includes, but is not limited to, records that are either stored or shared via electronic mail; including instant messaging for official business.

All employees must familiarize themselves with this email retention policy and the specific retentions relating to their department or division. Questions about the proper classification of a specific piece of information should be addressed to the Director of Human Resources.

This email retention policy is secondary to the SBCTC retention policy; any current public record requests for specific public records; and any litigation hold notices for records in response to potential litigation. The **sender** is responsible for retaining emails within the College. The **recipient** is responsible for retaining emails that originate outside the College.

Email retention is generally subject to the following retention periods (see the State Board record retention schedule):

- **Transitory administrative records**
Records which have no administrative, legal, fiscal, or archival requirement for their retention. These records include personal messages and announcements not related to business; information-only copies; copies of published materials; duplicate copies; preliminary drafts; internal requests for information; transmittal memos; reservations and confirmations; routine college admission letters. Retain until administrative need is satisfied.
- **Routine correspondence**
Routine correspondence concerning day-to-day office administration and activities. These records include intra-agency correspondence; routine correspondence with other agencies; and correspondence with the public on routine matters. This category does not include executive level correspondence or correspondence concerning policies and procedures. Retain for 30 days.

- **Executive level documentation**
These records include correspondence and memos at the executive level to and from public officials, the public, and others, concerning policy issues, concerns, actions, or issues. Retain for 4 years in Chief Executive's Office.
- **Non-executive level planning and working files**
These records include project design plans, survey forms, charges, diagrams, statistics, preliminary analysis reports, research materials, drafts, and other documentation related to management studies, non-fiscal audits, surveys, and planning studies. Retain for 2 years in originating office or designated office.

Encrypted Communications

E-mail, and any attachments, containing confidential information shall be encrypted from the sending device to the receiving device. The ability to un-encrypt sender's message through authorized process; sending organization must be able to un-encrypt and retrieve originating version of sent message.

Encrypted communications of confidential information should be stored in a manner consistent with College policy, but in general, information should be stored in a decrypted format unless it is confidential personnel, business, protected health or financial information. Please check with the College's Information Services to obtain the appropriate licensed encryption software.

Retention Mailboxes

Employees shall retain specific types of email records with longer retention period by copying or blind copying their correspondence to the following mailboxes. After the expiration period, the records may be transferred to archives.

Retention Mailboxes

- Accreditation email: accreditation@lowercolumbia.edu (retention period 6 years)
- Alumni fundraising: Alumni@lowercolumbia.edu (6 years after completion of project)
- Attorney General correspondence: Attorneygeneral@lowercolumbia.edu (6 years)
- Audit files: Audits@lowercolumbia.edu (3 years from completion of internal or external audit)
- Business records and contracts: Businessrecords@lowercolumbia.edu (6 years following termination of contract)
- Chief Executive Officer level correspondence: Admin@lowercolumbia.edu (4 years)
- Facilities requests: Facilitiesuse@lowercolumbia.edu (date of approval/non-approval plus 1 year)
- Formal student complaints: Studentcomplaints@lowercolumbia.edu (1 year following disposition of complaint)
- Legal issues: Legalissues@lowercolumbia.edu (6 years, then archive)
- Legislative contacts and lobbying: Legislative@lowercolumbia.edu (End of session plus 4 years)
- Newsletters: Newsletters@lowercolumbia.edu (2 years)
- Personnel records: Personnel@lowercolumbia.edu (up to 6 years after termination of employment)
- Planning and working files (administrative level) Planningfiles@lowercolumbia.edu (2 years)
- Policies and procedures: Policies@lowercolumbia.edu (6 years or until superseded)

- Public disclosure requests and responses: Publicrecordrequests@lowercolumbia.edu (final disposition plus 1 year)
- Public information requests and responses: Publicinformationrequests@lowercolumbia.edu (response plus 1 year)
- Rule making correspondence: Rulemaking@lowercolumbia.edu (until superseded plus 6 years)
- Student government agenda and minutes: ASG@lowercolumbia.edu (3 years then archive)
- Student clubs agenda and minutes: Studentclubs@lowercolumbia.edu (3 years then archive)


- **Adopted 11-30-2009**

Historic Review:

- Reviewed by the Cabinet and Leadership Team May 2009
- Campus Review: Oct. 26 - Nov. 6, 2009

Resources, References, Procedures, or contact information relating to this policy

Resource/Reference/Procedure	Title	Unit Responsibility
Procedure 705.1	E-Mail Retention Procedures	VP Administration/Director of Information Services
SBCTC E-mail Retention Policy		

	Chapter 7 – Information Systems and Services
Administrative Policy	ACCESSIBLE TECHNOLOGY POLICY POLICY 720

720 Accessible Technology Policy

Lower Columbia College provides equal opportunity to its educational and administrative services, programs, and activities in accordance with federal and state law. Equal opportunity includes appropriate and effective access to technology for students, employees, and community members.

This policy applies to the procurement, development and implementation of instructional, administrative, and communications technologies and content, unless it creates an undue burden on the college. It encompasses, but is not limited to, college websites, learning management tools, student information systems, training materials, instructional materials and assessment tools.

Ensuring equal and effective electronic and information technology access is the responsibility of all college administrators, faculty, and staff.


- **Adopted 5-22-17**

Resources, References, Procedures, or contact information relating to this policy

Resource/Reference/Procedure	Title	Unit Responsibility
Procedure 720.1A	Posting Documents to the Website	VP of SS
Procedure 720.2A	Accessible Technology Procurement Procedure	Director of IT
WA RCW 28B.10.912	Students with disabilities	
WA RCW 49.60	Discrimination-Human Rights Commission	
WA OCIO Policy 101	Technology Policies and Standards	
WA OCIO Policy 188	Accessibility	
SBCTC Policy 3.20.30b	SBCTC Accessible Technology	
	Americans with Disabilities Act of 1990 (ADA)	
	Amendments Act of 2008	
	Section 504 of the Rehabilitation Act of 1973	
	Section 508 of the 1973 Rehabilitation Act	
WCAG 2.0	Web Content Accessibility Guidelines (WCAG) 2.0	

Historic Review:

- Reviewed by Cabinet: January – March 15, 2017
- Reviewed by Leadership Team: March 16, 2017
- Reviewed by Union Management: March 21, 2017
- Reviewed by Faculty (represented by Lucas Myers): April 3-6, 2017
- Sent to UMCC, Governance Council, Operations Council, and Leadership: April 10-21, 2017
- Reviewed (2nd draft) – by Leadership Team: April 24, 2017
- Reviewed by Governance Council: May 3, 2017
- Campus Review: May 5-19, 2017
- Adopted by Cabinet: May 22, 2017

	Chapter 7 – Information Systems and Services
Administrative Policy	USE of ELECTRONIC SIGNATURES and SUBMISSION POLICY 725

725 USE of ELECTRONIC SIGNATURES and SUBMISSION

This policy is designed to provide reasonable assurance for the integrity, authenticity, and nonrepudiation of electronic documents when electronic signatures and submissions are used and accepted; and to promote the use of electronic signatures and submissions throughout Lower Columbia College (LCC).

This policy and its procedures apply to all LCC employees participating in the approval, selection, acquisition, and implementation of an electronic signature solution.

Background:

The use of electronic records and electronic signatures can significantly reduce costs, simplify transactions and speed up transaction time. Lower Columbia College (LCC) intends to promote electronic transactions and remove barriers that might prevent electronic transactions throughout the college. Changes to Washington law make it clear that organizations are allowed and encouraged to use and accept electronic signatures to authenticate electronic transactions. Unless otherwise specified by law, electronic signatures have the same force and effect as that of a handwritten signature.

State agencies must meet the following requirements in order to use and accept electronic signatures or electronic submissions:

State agencies are required to put in place by policy or rule, the methods and process for using or accepting electronic submissions or electronic signatures.

Electronic records and signatures must be consistent with policy, standards and guidelines provided by the state’s chief information officer.

To the fullest extent allowed by law, Lower Columbia College (LCC) encourages electronic transactions and recognizes electronic records and signatures. The use and acceptance of electronic signatures and electronic submissions/records shall be consistent with the guidance and requirements put in place by the Office of the Chief Information Officer (OCIO).

The Vice President of Administrative Services in consultation with the Director of IT Services and the Finance Director shall approve specific methods and processes for electronic signatures and submissions. These approval authorities may be delegated at the discretion of the VP of Administrative Services.

The approval of solutions shall be coordinated through the IT Services department. The VP of Administrative Services shall determine a suitable review and approval process to be used when determining which solution(s) are suitable for a particular type of record or transaction. Where appropriate, a team approach shall be used.

Approved solutions shall be listed in the related procedures.

This policy and changes to this policy shall be made available on the OCIO website and the DES Laws, Rules, and Policies website.

Definitions:

Electronic Signature: An electronic signature is a sound, symbol, or process attached or associated with an electronic record and executed or adopted by a person with the intent to sign the record. The integrity and authenticity of a record with an electronic signatures needs to be preserved over time. Signatures are used when:

- required by law, or
- the significance of a transaction needs to be emphasized, or
- the transaction needs to be bound to a person

In practice, electronic signatures emphasize one or more of the following four parts:

- the identification and authentication of the signer, or
- the intent to sign, or
- the association of the signature to the record, or
- the authenticity and integrity of the record

Authentication: The assurance that an electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.

Authorization: When an individual has both verified permission and the requisite authority to sign a record, access specific college services, or perform certain operations, including executing binding agreements.

Electronic Record: A record created, generated, communicated, sent, received, or stored by electronic means.

Nonrepudiation: Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Record Integrity: Integrity refers to the assurance that a record is preserved without any alteration that would impair its use as an authentic record. Both accuracy and the completeness of the electronic record must be preserved.

Click Through or Click Wrap: In this type of electronic signature, a signer is asked to affirm his or her intent or agreement by checking a box or clicking a button. The Click Through/Click Wrap approach is commonly used for low risk, low value consumer transactions.

Password or Personal Identification Number (PIN): When using a password or PIN for an e-signature, a person is required to enter identifying information, which may include an identification number, the person's name and a "shared secret" such as a PIN or password. A password/PIN is more secure than the click through/click wrap method.

Digitized Signature: A digitized signature is a graphical image of a handwritten signature. This approach may use specialized hardware or software for additional security. A digitized signature is more secure than the password/PIN method.

Digital Signatures: A “digital signature” is created when the signer uses a private signing key to create a unique mark (called a “signed hash”) on an electronic document. The recipient of the document uses the signer's public key to validate the authenticity of the private key and to verify that the document was not altered after signing. A digital signature is more secure than the digitized signature method.

Hybrid Approaches: Hybrid electronic signature solutions are available by combining techniques from various approaches to provide increased security, authentication, record integrity and non-repudiation.

Resources, References, Procedures, or contact information relating to this policy

<ul style="list-style-type: none"> • Procedure 725.1A – Use of Electronic Signatures and Submission Procedures 	VP Administration and Director of IT
<ul style="list-style-type: none"> • Electronic Signatures in Global and National Commerce Act (E-Sign Act) • Title IV of the Higher Education Act of 1965 (HEA) • Standards for Electronic Signatures in Electronic Student Loan Transactions (US Dept. of Education) • Washington DES Laws, Rules, and Policies website • Washington OCIO Electronic Signature Guidelines • Washington OCIO Links to Agency Electronic Signature or Record Policies website • Washington RCW Title 19, Chapter 19.360 	

- Reviewed by the Cabinet November 2017
- Reviewed by Governance Council 12/6/17 –(Recommended taking to UMCC and Operations Council, then proceed with campus review)
- Reviewed by Operations Council 12/11/17
- Reviewed by UMCC 1/16/18
- Campus Review 1/18/18 – 2/2/18
- Governance Council Review 2/7/18
- **Approved by the Executive Leadership Team 2/7/18**