COLLEGE of CHARLESTON

OFFICIAL POLICY

10.14	Electronic Communications Usage Policy	08/23/16

Policy Statement

Campus policy detailing accepted use, limits and retention of electronic communication.

Policy Manager and Responsible Department or Office

Chief Information Security Officer, Information Technology

Purpose/Reason for the Policy

The purpose of this policy is to present guidelines relating to the responsibilities, legal obligations and permissible use of the College's electronic communication tools. The College of Charleston is committed to providing effective tools to allow greater efficiency in communication. The appropriate use of electronic communication tools in support of the College's teaching, research, administrative and service functions is outlined in this document -- including usage, limits, confidentiality, ownership and enforcement.

Departments/Offices Affected by the Policy

All faculty, adjunct, staff, retirees, students, student workers, alumni, temporary workers, contractors and affiliates operating on behalf of the College of Charleston are required to comply with the policy and are bound by law to observe applicable statutory legislation. This policy covers appropriate use of all electronic communication tools owned or operated by the College.

Procedures Related to the Policy

This policy addresses Electronic Communications:
Current tools include but are not limited to :

- Electronic Mail
- Instant Messaging
- ListServ
- Forums
- Collaboration/social media tools

Purpose and Usage of Electronic Mail
Electronic Mail (aka "Email") is the primary communications tool used to disseminate information and alerts to all faculty, staff and students. Email accounts and services are provided to all faculty, staff and students of the College. Email messages are part of the College's official records of work and must be treated accordingly. Communications and email systems are property of the College of Charleston and State of South Carolina.

Purpose and Usage of Instant Messaging
Instant Messaging (aka "IM" or "Online Chat") is a tool provided by the College of Charleston to all employees to see current availability of others on campus and to facilitate a real-time, online conversation or videoconference. Each user account has access to this tool; however, department policy determines availability of the tool.

Purpose and Usage of the ListServ, Forums and Collaboration/Social Media Tools
The College provides forums, listservs and other collaborative/social communications tools for all electronic communication that is not official College business. This includes but is not limited to special groups, events, discussions, debates, and personal commentary. The College does not exercise censorship or pre-screen messages. The College has no control over the quality, safety or legality of the information posted, nor the truth, accuracy or reliability of the information posted. Users are solely responsible for the form, content and accuracy of any submission placed by that user. The College will, however, conduct investigations of individual complaints about misuse of these communication tools.

Electronic Communications Standards

Electronic communications are unsecure and therefore shall not be used for the following purposes:

- communications or storage of information including confidential or protected information (FERPA, HIPPA or other PII data)
- to send or forward unsolicited communications ("spam")
- to access or disclose another person's communication contents without proper authorization
- for personal financial gain
- to violate College policy including the Privacy Policy or related codes of conduct (harassment/cyber bullying)
- for unlawful activities
- to communicate support or opposition of political devotions including, but not limited to statements, opinions, or solicitations
- communications supporting any business function that is not directly in support of College business functions and procedures
- to send sensitive, libelous or abusive content

Authorized Usage

- At no time should users share their individual access with anyone unless permission granted by supervisor.
- At no time should users attempt to use the account privileges of others.
- Department or Shared accounts must be accessed utilizing the users own credentials via additional permissions. Authorized users of a departmental account will have the ability to reply from that account.
- At no time should users misrepresent the College or their own identity
- The College's email system is provided for College business only
- All data must comply with copyright and fair use laws

Operations and Security

Forwarding

To protect FERPA, HIPPA and PII data that may inadvertently exist in email accounts -- forwarding rules that forward all mail from a campus account to an outside email service provider such as Gmail is not permitted. It is permissible to forward individual messages manually to an outside email account after a user has confirmed that the message does not contain protected data.

Authentication, Confidentiality & Remediation

Authentication

The College does not guarantee the authentication or integrity of email, instant message, forum post or listserv message.

Confidentiality
Confidentiality of electronic mail, instant messaging, ListServ and Forums cannot be assured.

Compromised Account Remediation
Accounts that have been compromised will be immediately suspended until investigation and remediation occur. A suspended account will have no access to any network related services. Users will be required to change passwords and take or re-take the phishing quiz to regain account privileges.

Retention & Right of Access
When employees leave the College, communication accounts are suspended on the last day of employment or expiration of contract terms. Accounts are terminated and removed from college systems 30 days from the last day of employment or contract expiration date. Requests for retaining accounts should be sent to Helpdesk (Helpdesk@cofc.edu).

Information Technology reserves the right to disable communication accounts that are found in violation of College policy or that negatively impacts the College's electronic services performance, or that threaten the security of the College's networks.

Violations
Violation of any portion of this policy may result in immediate loss of access to College of Charleston IT assets, initiation of legal action by the College of Charleston, and/or disciplinary action as appropriate. All users are responsible for reporting any actual or suspected violation of this policy to the College of Charleston Information security officer immediately.

Related Policies, Documents or Forms

Privacy Policy
Data Loss Prevention Policy
Acceptable Use Policy

Review Schedule

Issue Date:8/23/2016 **Date of Policy Revision:8/23/2016**	**Next Review Date:10/23/2020**

POLICY APPROVAL
(For use by the Office of the Board of Trustees or the Office of the President)

Policy Number: 10.14

President or
Chairman, Board of Trustees  Date: 9-23-16