(The Senate and Senate Committees should use the following form for officially co
recommendations to the Provost. Such committees would include: UCC, UPC and
Senate along with any other committees which provide recommendations directly t

Copies mailed out on 11/26/12.

Senate Recommendation to the Provost

Originating Body: Faculty Senate

Originator: Faculty Welfare Committee

Date Submitted: 11/20/2012 Requested Effective Date: ASAP

Recommendation: Salisbury University Electronic Mail Services Acceptable Use Policy
Acceptable Use of Computing and Electronic Recources

Date Approved by Senate: 11/13/2012

Craig Clarke 11/28/12

President, Faculty Senate Date

Attach any supporting documentation. **See Attached Document**

Action Taken by Provost: **Date** 11-26-12

✓ Recommendation Accepted ____ Recommendation Not Accepted

____ Recommendation returned to Originating Body for further review (see attached)

Disposition for Approved Recommendation:

____ President
✓ Faculty Senate President
____ Forum Chair
✓ Webmaster
____ Catalogue Editor
____ VP Student Affairs
____ VP Finance
✓ School Deans
____ Graduate Council
✓ Provost Council
✓ Ken Kundell

Diane D. Allen 11-26-12

Provost Date

Acceptable Use of Computing and Electronic Resources
Salisbury University

I. Purpose

The purpose of this policy is to outline the standards for responsible and acceptable use of Salisbury University ("University") computer and information technology ("IT") resources. In support of the University's mission, IT resources are provided to Authorized Users related to their University status and responsibilities to support the academic, research, instructional, administrative, service and otherwise educational endeavors of the University. The University is committed to Constitutional First Amendment principles of free expression and the fundamental liberal arts concept of scholarly inquiry and free exchange of ideas. The University will not engage in censorship or otherwise limit access to information when the content is legal. Each Authorized User is expected to conduct oneself and one's use of University IT resources responsibly, ethically, in compliance with the law and the rights of one another. Inappropriate use of IT resources exposes the University to risks including, but not limited to, breach of personal computer security, exposure of restricted data, compromise of network systems and services, detriments to technology performance, breach of University contracts, and legal liability. Information Technology ("IT") is committed to protecting Authorized Users and the University from intentional or negligent illegal or damaging use of IT resources.

II. Definitions

a. Authorized Users. Authorized Users include the following categories of University affiliated entities:
   i. University residential students, commuting students and their guests while on the University campus;
   ii. University employees, including faculty, staff, student employees, temporary and other categories of University workers; and
   iii. Contractors, consultants, and all personnel affiliated with third parties under contract with the University.

b. Information Technology Resources. IT resources include, but are not limited to, University owned or leased Electronic Equipment, operating systems, storage media, applications, software, files and network accounts providing electronic mail, web browsing and file transfer.

c. Electronic Equipment. Electronic equipment includes, but is not limited to, laptop and desktop computers, tablets, mobile and smart phones, personal digital assistants, scanners, printers, flash drives, data/memory sticks and docking stations.

III. Scope

This policy applies to Authorized Users who use and/or access the IT resources whether on the University's campus(es), off campus, or through virtual personal networks. This policy applies to all equipment that is owned or leased by the University and governs activity on personal devices while on the University campus that utilizes any IT resources as well as all communications to and from the University while off campus. The

University generally does not monitor material residing on University computers housed within a private residence or on non-University computers, regardless of whether such computers are attached or able to connect to campus networks.

IV. General Use and Ownership

IT resources are the property of the State of Maryland and the University. Authorized Users may use IT resources for incidental personal use and in support of the business and academic mission of the University. It is the responsibility of each Authorized User to know and comply with this policy and security standards published by IT. This responsibility includes protecting the privacy and security of passwords, and using IT resources solely for their intended purposes. Authorized Users are solely responsible for their use of IT resources, and may not represent or imply that their associated use constitutes the views or policies of the University. Communications originating from the Authorized User are identified as such and the Authorized User assumes responsibility for all communication originating from equipment or accounts assigned to that User. In the event of a security breach related to User accounts or equipment, the User shall act expeditiously to report and correct the situation.

Authorized University IT officials may monitor and access systems, network traffic and Electronic Equipment for maintenance, operation, security, quality of service, business-related purposes (such as audits), to investigate an alleged violation of this policy, and for policy or legal compliance. An Authorized User's privacy will be preserved to the extent possible, subject to the University's administrative, business and legal obligations. There should be no expectation of privacy in the material sent or received when using IT resources or third party vendor applications provided by the University (e.g. student email systems). All data created or received for work purposes and contained in University electronic files, servers or email are public records, unless otherwise protected by law or contract. All public records shall be maintained and disposed in compliance with State, USM and University approved record retention and disposition schedules.

USM Records Retention Standards

V. Unacceptable Use

The use of IT resources is a privilege, not a right. Access is granted to Authorized Users subject to all University, University System of Maryland ("USM") and State of Maryland policies, Federal, State and local laws and ordinances. The following list, while not exhaustive, describes conduct defined as unacceptable use prohibited by this policy.

a. Knowingly using IT resources for illegal activity including, but not limited to,
    i. Sexual harassment;
    ii. Discrimination on the basis of a Federally protected characteristic or sexual orientation;
    iii. Infringing upon (i)Intellectual property rights, including Federal copyright law, trademark, patent, trade secret or software licensing, such as pirating, installing, copying, distributing, or using digital content such as software, music, text, images or video without appropriate license or as qualifies under "Fair Use;"

iv. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. Legal counsel and appropriate administration should be consulted prior to export of any material in question;
v. Obscenity;
vi. Child pornography;
vii. Threats or harassment by means of email, instant messaging, telephone or paging, whether through language, frequency or size of messages;
viii. Defamation; or
ix. Theft, including identity theft.

b. Unauthorized access, altering or reverse engineering system software or hardware configurations
c. Deliberately or knowingly (d)Disrupting, interfering with, or denying service to any Authorized User or IT service administration, including overloading or otherwise adversely impacting system performance and support, regardless of whether the conduct actually impacts other Authorized Users' use of the IT resources
d. Accessing, attempting access, or facilitating access to another User's accounts, private files, email messages, or intercepting network communication without the User's permission, except in accordance with job responsibilities for legitimate University purposes
e. Misrepresenting oneself as another individual electronically
f. Any effort, regardless of whether successful, to circumvent IT system security
g. Use for commercial gain or private profit, including running a non-affiliated University business or personal consulting outside the scope of University job responsibilities, except as permitted by University intellectual property policies or University spinoffs endorsed and managed through University research and technology transfer offices
h. Representing oneself as an agent of the University without authority
i. Accessing and/or disclosing sensitive or confidential information without authority
j. Intentionally or recklessly introducing or transmitting destructive or malicious programs such as viruses into the network or networked devices
k. Allowing use of Authorized User's or other accounts by others, including family and other household members. Circumventing user authentication or security of any host, network or account
l. Forwarding restricted University email to unauthorized recipients
m. Sending or posting unsolicited and/or inappropriate mass email messages without proper authorization; examples of unacceptable use include "spam" junk email, chain letters, pyramid schemes or other commercial advertising
n. Unauthorized use, deliberate disguising of the sender, or forging of email header information, including alteration of the content of an email message originating from another sender with an intent to deceive

VI. Enforcement

A violation of this policy constitutes unacceptable use of IT resources and may violate other University policies and/or federal or state law. Known or suspected violations of this policy should be reported to IT. The University Chief Information Officer ("CIO") or his/her designee may suspend, block, relocate to a secure site, or restrict access to information and network resources when necessary to protect the integrity, security or functionality of IT resources or to protect the University from liability. Notice of any such action will be provided to the Vice President for the affected unit. Appropriate University officials and/or law enforcement agencies will respond to any alleged violations of this policy. Authorized Users in violation of this policy may ~~result in~~ be subject to restriction, suspension or termination of access to computing accounts, the network or other IT resources and/or other University owned technology devices as well as disciplinary action as defined in, but not limited to, the Student Code of Conduct, the Faculty Handbook, Policy Manual for Employees, University contracts and State of Maryland, USM and other University policies. A violation of this policy may constitute an alleged criminal offense and may also be referred for criminal or civil prosecution under applicable Federal and/or State law(s).

VII. Review

Consistent with USM requirements, this policy will be reviewed and updated annually or as needed based on the recommendation of the CIO. Such updates will be conducted in a manner consistent with the practices of shared governance. All updates made will be reported to the governance bodies (i.e. Staff, Student and Faculty Senates).

VIII. Links to Related USM and SU Policies

Guidelines in Response to the State IT Security Policy and Standards

IX. Contact

To report comments, questions or an alleged violation of this policy, please contact the Policy Administrator: abuse@salisbury.edu
Salisbury University Information Technology
Teacher Education & Technology Center, Room 201
(410) 543-6111

X. Approved: August 1, 2012

Salisbury University Electronic Mail Services Acceptable Use Policy*

GENERAL PRINCIPLES

Electronic mail (email) services at SU are provided to support education, personal and scholarly communication, administration and other SU business. Everyone using email should be considerate of the needs of others, and be certain not to impede the use of the email services by others. Users should be respectful of the feelings of others and be aware that any message can be redistributed to anyone with great ease. In addition, all electronic messages must contain the name and electronic mail address of the person making the information available; no anonymous information should be sent.

Email access is provided for all students, faculty and staff of the university. For students, email access remains in place for two years following their separation from the university. Faculty and staff are provided email services while they are employed by the university. Exceptions are made for faculty and staff who retire from the university. Their access to email is continued for one year intervals. They will be asked annually if they would like to continue using email.

EMAIL PRIVACY

Electronic mail messages are considered private correspondence. As such, messages are viewed as the private property of the receiver and will not be made available to other members of the campus community without the owners' consent. Although privacy and security are of the utmost importance, university administrators may access messages under some circumstances. These include:

- To comply with a request under federal or state public information laws;
- To maintain, repair, and trouble shoot the computer network;
- To investigate misuse of the network, such as theft, copyright infringement, gambling, pornography, and harassment, after the University is put on notice of a specific concern; and
- To obtain university business records and to conduct business-related investigation, such as audits.

ACCEPTABLE USES OF UNIVERSITY EMAIL

The SU email system may be used as follows:

- To perform educational/university business and to communicate with all friends, family, classmates, and associates locally and off campus.
- To communicate with local and foreign educators, students, researchers and colleagues in connection with instruction or research.

UNACCEPTABLE USES OF UNIVERSITY EMAIL

The SU email system may not be used:

- To engage in or promote a private commercial business purposes in violation of University policies**;
- To send chain letters, or any illegal schemes or activities;
- To send mailings to large numbers of people that contains unwanted solicitations or information. These mailings are often referred to as "spam." (The university provides a daily Campus Bulletin Digest that should be the vehicle for the distribution of general interest information);
- To launch an email "attack" resulting in a denial of service to university email users;
- To send messages which constitute illegal activities or harassment or infringement on the rights of others;
- To send anonymous mailings, or mailings which impersonate another individual;
- To introduce a computer virus; or
- To violate the constraints on communications imposed by any licensing or professional association to which the user belongs.

ENFORCEMENT OF POLICY

Any user, who engages in the actions specifically prohibited under "Unacceptable Uses," as judged by the University Chief Information Officer, may lose access to e-mail services, pending a meeting with the Chief Information Officer. Notification of loss of access must be accompanied by a written explanation. If the issue is not resolved during this meeting, further appeal may be necessary to regain email access. In the case of students, the Office of the Vice- President of Student Affairs will determine the appropriate action including referral to the University Judicial System. In the case of faculty, the Academic Freedom and Tenure Committee will make the judgment and in the case of staff, the appropriate supervising Vice President will hear any appeal.

CAMPUS BULLETIN DIGEST

The University maintains a list server that disseminates non-business related information to interested users on a daily basis. The Campus Bulletin Digest (CBD) compiles emails from users and sends these items in the form of one email message a day. Users may subscribe or unsubscribe from the Digest, at will. Personal or non-business matters should be distributed through the Digest rather than through email messages to everyone on Campus. Submissions to the Campus Bulletin Digest must follow the same acceptable use requirements as any other campus email.

RECOMMENDATIONS ON EMAIL USE

Some recommendations for the use of campus email:

1. It is recommended that communication of confidential or proprietary information be restricted as much as possible.
2. If a user inadvertently comes upon information not intended for public viewing, exit immediately.
3. It is recommended that users store no personal information about others in their files.
4. Files that are considered highly personal or confidential should be stored on the owners' personal computer and protected by a password, and removed from the campus network.
5. It is strongly recommended that users maintain the confidentiality of their email and network passwords. Approved by SU Faculty and staff Senates Spring 2002.

*This policy does not supercede or negate any part of the SU Information Technology Acceptable Use policy available at http://helpdesk.salisbury.edu/documents/policies/AcceptableUsePolicy.doc.

**To use the system for non-University public relations or non-profit fund-raising activities, forward information to the Public Relations Office. (Comprehensive list will be published regularly and used in weekly campus-wide newsletter, eSU News.)