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 (³8QLYHUVLW\´ FRPSXWHU DQG LQIRUPDWLRQ resources. , Q VXSSRUW RI WKH 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

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. $Q $XWKRUL]HG 8VHU LV FRQVHQWLQJ WR the extent WR SRVVLEOH VXEMHFW WR 8QLYHUVLW\ 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:
http V://www.salisbury.eduDGPLQLVWUDWLRQ DGPLQLVWUDWLRQ DQ WHFKQRORJ\ LQIRUPDWLRQ SROLFLHV Policies USMRecordsRetentionStandards.pdf

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 0DU\ODQG ³860´ DQG 6WDWH 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. Intellectual property rights, including Federal copyright law, trademark, patent, trade secret or software licensing, such as pirating, installing,

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 rep R U W H G W R , 7 7 K H 8 Q L Y H U V L W \ & K L H I , Q I 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 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