


**Coppin State University  
Information Technology Division  
Policies and Procedures**

<b><u>Policy #:</u></b>	<b>ITD – GEN – 006</b>	<b>Version: 02</b>
<b><u>Subject:</u></b>	<b>CSU Faculty/Staff Computer Use and Internet Access Policy</b>	<b>Effective Date: 07/01/2011</b>
		<b><u>Approval Date:</u> 08/01/2018</b>
<b><u>Approved by:</u></b>		<b><u>Review Date:</u> 08/01/2018</b>

---

## **I. Purpose**

To establish a policy to ensure the proper use of Coppin State University’s computer and network resources and services by its employees, students, independent contractors and other computer users. All computer and network users have the responsibility to use these resources in an efficient, effective, ethical and lawful manner.

The following policy, rules and conditions apply to all users of computer and network resources and services, including Internet resources, wherever the users are located. It applies to all computer and Internet communication facilities owned, leased, operated or contracted by CSU.

It is intended to encompass and conform to the Internet Access and Security Policy Guidelines of the State of Maryland (“State”). Violations of this policy may result in disciplinary action, including possible suspension, termination, and/or legal action. More specific policies relating to student use are addressed in a separate document.

Violations will be forwarded to the Office of Human Resources, for staff, or the Office of the Provost, for faculty, and will be adjudicated in accordance with the current procedures.

Violations may result in revocation of computing resource privileges, faculty/staff disciplinary action or legal action.

## **II. Policy**

### ***Introduction***

Coppin State University has the right, but not the duty, to monitor any and all aspects of the computer system, including employee or student e-mail, to ensure compliance with this policy.

The computers and computer accounts given to employees and students are to assist them in the performance of their jobs or the furtherance of their studies. Employees and students should not have an expectation of privacy in anything they create, send, or receive on the computer. The computer and network systems belong to Coppin State University and may be used for its business or educational purposes only.

#### ***External Conditions of Use***

Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

#### ***Equipment***

Computer users are governed by the following provisions, which apply to all use of computer and telecommunication resources and services. Computers and network resources and services include, but are not limited to the following: host computers, servers, workstations, standalone computers, laptops, software, printers, and internal or external communications networks (Internet, commercial online services, bulletin board systems, and e-mail systems) that are accessed directly or indirectly from Coppin State University's computer facilities.

#### ***Revisions***

This policy may be amended or revised periodically as the need arises.

### **III. Procedure**

#### ***Responsibilities of Users***

Access to the CSU network and to Internet resources infrastructure both within and beyond CSU campus, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community.

The term "users," as used in this policy, refers to all employees, independent contractors, students and other persons or entities accessing or using Coppin State University's computer and telecommunications resources and services. Coppin State University is not responsible for the actions of individual users.

#### ***Copyrights and Licenses***

Users must comply with all software licenses, copyrights and all other state and federal laws governing intellectual property. Users may not install software onto the network without first receiving express authorization to do so from the Vice President of the Information Technology Division.

- Copying - All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any CSU facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.
- Number of Simultaneous Use - The number and distribution of copies must be handled in such a way that the number of simultaneous users does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.
- Copyrights - In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media

### ***Integrity of Information Resources***

Computers users must respect the integrity of computer-based information resources.

- Modification or Removal of Equipment -- Computers users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.
- Encroaching on Others' Access and Use - Computer users must not encroach on others' access and use of CSU's computers. This includes but is not limited to: the sending of chain-letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification for system facilities, operating systems, or disk partitions; attempting to crash or tie up a CSU computer or network; and damaging or vandalizing CSU computing facilities, equipment, software, or computer files.
- Unauthorized or Destructive Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system and/or damage the software or hardware components of the system.

Computer users must use great care to ensure they do not use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than permitted in network guidelines. The use of any unauthorized or destructive program may result in criminal or civil action.

### ***Unauthorized Access***

A user's ability to connect to other computer systems throughout the network does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems. Computer users must refrain

from seeking to gain unauthorized access to information resources or enabling unauthorized access.

- Abuse of Computing Privileges - Users of CSU information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether computer, software, data, information, or network in question is owned by CSU. For example, abuse of the networks to which CSU belongs or the computers at other sites connected to those networks will be treated as an abuse of CSU computer privileges.
- Reporting Problems - Any defects discovered in system accounting or system security must be reported to the Information Technology Division so that steps can be taken to investigate and solve the problem.
- Password Protection - Users are responsible for safeguarding their passwords for the system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the Vice President of the Information Technology Division.

### *Privacy*

Most State systems provide mechanism for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to private information are a violation of CSU policy and may violate applicable law. Authorized system administrators may access computer users' files at any time for maintenance purposes. System administrators will report suspected unlawful or improper activities to the proper authorities.

- Unlawful Messages - Use of electronic communication facilities (such as mail or talk, or systems with similar functions) to send fraudulent, harassing, obscene, threatening or other messages that are a violation of applicable federal, state, or other law or STATE or CSU policy is prohibited. Users encountering or receiving such material should immediately report the incident to their supervisor.
- Mailing Lists - Users must respect the purpose and charters of computer mailing lists (including local network newsgroups and bulletin-boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the list's purpose. Persons sending to a mailing list any materials which are not consistent with the list's purpose will be viewed as having sent unsolicited material.
- Advertisements - In general, CSU's electronic communication facilities should not be used to transmit commercial or personal advertisements, solicitations or promotions (See Commercial Use, below). Some public bulletin boards have

been designated for selling items, etc., and may be used appropriately, according to the stated purpose of the list(s). Vendors may send product information and technical material to specific mailing lists, with the permission of the manager of the mailing lists.

- Information belonging to others - users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those users.
- Confidentiality - CSU does not exist in isolation from other communities and jurisdictions and their laws. Under certain circumstances, as a result of investigations, subpoena or lawsuits, individual users or CSU may be required by law to provide electronic or other records or information related to those records or relating to use of information resources.

#### ***Political, Personal and Commercial Use***

- Political use - CSU information resources must not be used for partisan political activities where prohibited by federal, states or other applicable laws, and may be used for other political activities only when in compliance with federal, state and other laws and in compliance with applicable STATE and CSU policies.
- Personal use - CSU information resources should not be used for personal activities not related to appropriate CSU functions, except in an incidental manner.
- Commercial use - CSU information resources should not be used for commercial purposes except in a purely incidental manner or as permitted under other written policies of CSU or with the written approval of a CSU officer having the authority to give such approval. Any such commercial use should be properly related to CSU activities, take into account proper cost allocations for government and other overhead determinations and provide cost allocations for government and other overhead determinations and provide for appropriate reimbursement to CSU for taxes and other costs CSU may incur by reason of the commercial use.

#### ***Internet Access and Use***

The Internet is a powerful medium for information dissemination and gathering. Because of the immense variety of information accessible from anywhere in the world, and the freedom of speech supported by the internet, CSU, as owner of the CSU servers, must determine guidelines for appropriate content and format that meet its standards of professionalism. Adherence to these guidelines is prerequisite to continued use of the CSU servers.

#### **IV. Definitions**

The following terms apply for the purpose of this policy. Definitions for these terms may be found at <https://lookup.coppin.edu/cpd/Pages/Home.aspx>:

[Academic Content](#)

[Acceptable Risk](#)

[Accountability](#)

[As Needed Basis](#)

[Authentication](#)

[Authorization](#)

[Authorized Software](#)

[Certification](#)

[Computer](#)

[Confidentiality](#)

[Cookies](#)

[Copyright](#)

[Course Site](#)

[Data Owner](#)

[DMCA](#)

[DMZ](#)

[Firewall](#)

[HEOA](#)

[Incident](#)

[Information Custodian](#)

[Initial password](#)

[Integrity](#)

[IP Address](#)

[IT Systems](#)

[Mobile Code](#)

[Mobile Device](#)

[Microsite](#)

[Network](#)

[Non-Public](#)

[Non-Sensitive Information](#)

[OIT](#)

[Password](#)

[Peer-To-Peer File Sharing](#)

[Policy](#)

[Privacy](#)

[Protected Resource](#)

[Public](#)

[Risk](#)

[Sensitive Information](#)

[Smart Classroom](#)

[Software](#)

[Storage Media](#)

[Student](#)

[Student Organization](#)

[Support](#)

[Term Activation](#)

*Trusted Entity*

*Vendor*

*Universal Resource Locator (URL)*

*Version*

*Un-trusted Entity*

*Virtual Machine (VM)*

*Upgrade*

*VoIP*

## **V. References**

- Policy: ITD-CNS-002, CSU System Monitoring Policy
- Policy: ITD-CNS-003, CSU Firewall Policy
- Policy: ITD-GEN-004, CSU Illegal File Sharing Prevention Policy
- Policy: ITD-GEN-005, CSU Student Computer Use and Internet Access Policy
- Policy: ITD-GEN-011, CSU IT Security Program
- Policy: ITD-CNS-012, CSU Intrusion Prevention and Detection
- Procedure: ITD-GEN-007P, Incident Response Procedure