Acceptable Use of Technology Resources

This policy outlines the standards and expectations for responsible and acceptable use of college computing systems and information technology (IT) resources. The college provides access to technology resources in support of the mission of the college. The college's IT department is committed to protecting authorized users, computing systems, data, electronic communications and information technology resources from intentional or negligent illegal or damaging use. All users of the college's technology resources are expected to act responsibly, ethically and lawfully.

This policy applies to all employees, students, visitors and agents of the college who use and access the college's information technology resources, whether on campus, off campus or via remote connection. This policy applies to all equipment either owned or leased by the college and governs activity on personal computing devices while utilizing and/or accessing any college computing system or information technology resource.

The granting of privileges to use college computing systems and IT resources is predicated on the authorized user's acceptance of and adherence to the corresponding conditions and user responsibilities detailed in this policy. College resources should be used for business and academic purposes. Occasional, limited and appropriate use of college resources for personal use is permitted if that use does not interfere with the user's work performance. Authorized users assume responsibility for all communications originating from equipment or accounts assigned to the user. Authorized users are solely responsible for the use and handling of data, computing systems and information technology resources. It is the responsibility of all users to know the guidelines stated in college policies and to conduct their activities accordingly.

Information security is the responsibility of all users and any inappropriate use or suspected security incident must be reported to the college's IT department by calling 410-334-2870 or by emailing itinfo@worwic.edu. Authorized users agree to be good stewards when storing, accessing and transporting data.

The use of IT resources is a privilege and not a right. Under no circumstances are authorized users permitted to engage in any activity that is illegal. The following list of prohibited activities, by no means exhaustive, is an attempt to provide a framework for actions that fall into the category of unacceptable use:

- Using a computer without authorization;
- Obstructing the operation of the college's technology resources, including, but not limited to, intentionally damaging equipment, tampering with cables, adding or deleting files or software without authorization, and changing network settings;
- The intentional introduction or creation of invasive software, such as worms or viruses, Trojan horses and email bombs;
- Attaching a network device to the college's networks without approval of the IT department, including hubs, switches, wireless access points, routers or similar devices;

- Using computing systems, college networks or any other information technology resource to threaten or harass others or attempting to alter computer systems, hardware, software or account configurations;
- Monitoring another individual's account(s), data, communications, software, computing resources or email without prior consent;
- Sharing user account passwords with others;
- Allowing the use of an authorized user account by others, such as another family member or friend;
- Misrepresenting one's identity or role in any type of electronic communication;
- Using computing systems or information technology resources for commercial or profit-making purposes without written authorization from the college;
- Copying software found on college systems that is licensed by the college for personal use, transferring software to non-college equipment or modifying it in any unauthorized manner;
- Installing or operating computer games on college-owned computers for purposes other than academic instruction;
- Producing and broadcasting hate mail, discriminatory remarks or chain letters;
- Breaching or attempting to breach computer systems or information technology resources or security systems, whether with or without malicious intent;
- Engaging in any activity that can be harmful to systems or to any stored information, such as creating or propagating viruses or other types of malware;
- Violating copyright and/or software license agreements or downloading, installing or using illegal software;
- Installing or using any covert video/audio recording device; • Displaying any material that is sexually-explicit or discriminatory in nature; and
- Accessing or disclosing sensitive information without authorization or any theft of college data or equipment.

Authorized IT employees reserve the right to monitor and access any computing system or resource connected or attached to the college's networks. Monitoring can include, but is not limited to, reviewing, copying and accessing or archiving any information, logs, packets or other materials stored on, transmitted through or created with college technology resources. There is no expectation of privacy with regard to the college's computing systems, information technology resources and network infrastructure, while on or accessing resources remotely.

Violations of this policy are subject to college disciplinary procedures, state, local and federal laws and regulations. Based on the nature of the offense and/or the number of violations, employees and other agents of the college are subject to appropriate personnel action, up to and including dismissal. Students are subject to disciplinary action taken in accordance with procedures that govern student conduct, up to and including permanent suspension. If appropriate, the college can pursue criminal and civil prosecution.