Acceptable Use of Technology Resources

Scope and Purpose

This policy outlines the standards and expectations for responsible and acceptable use of college computing systems, cloud-based services and information technology (IT) resources. The college provides access to technology resources in support of the mission of the college. 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.

In general, acceptable use means ensuring that the information resources and technology of the college are used for their intended purposes. 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. It is the responsibility of all users to know the guidelines stated in college policies and to conduct their activities accordingly.

Responsibilities

The use of IT resources is a privilege and not a right. Authorized individuals assume responsibility for all communications originating from equipment or accounts assigned to them. Authorized users are solely responsible for the use and handling of data, computing systems and information technology resources.

Prohibited Conduct

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:

1. Altering system software or hardware configurations without authorization;
2. Disrupting or interfering with the delivery or administration of IT resources;
3. Causing network disruptions or unneeded network congestion;
4. Attaching network devices, such as switches, routers, hubs, access points, cameras, recording devices, without authorization;
5. Attempting to access or accessing another account, private files, email messages or intercepting network communications without authorization;
6. Misrepresenting oneself as another individual in electronic communication;
7. Installing, copying, distributing or using digital content (example: software, text, images and video) in violation of copyright and/or software agreements or applicable state and federal law;

8. Engaging in conduct that interferes with others' use of shared IT resources;
9. Using college IT resources for commercial or profitmaking purposes or representing interests of groups unaffiliated with the college or associated with normal academic, professional or business activities without authorization from the college;
10. Ignoring college or individual department policies, procedures or protocols;
11. Facilitating access to college IT resources by unauthorized users;
12. Exposing sensitive or confidential information or disclosing any electronic information that one does not have the authority to disclose;
13. Intentionally introducing or creating invasive software or malware;
14. Knowingly using IT resources for illegal activities, which may include obscenity, pornography, child pornography, threats, harassment, copyright infringement, college trademark infringement, defamation, theft, identity theft and unauthorized access;
15. Monitoring another user's account, data or communications, without prior consent or authorization;
16. Sharing user account passwords.

Security and Monitoring

The college's IT department is committed to protecting authorized users, computing systems, data, electronic communications and information resources from intentional or negligent illegal or damaging use. Information security is the responsibility of all users and any inappropriate use or suspected security incidents must be reported to the IT Help Desk by calling 410-334-2870 or emailing infosec@worwic.edu. Authorized users agree to be good stewards when storing, accessing and transporting college-owned data.

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, accessing or archiving any information, such as 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.

Enforcement

Violations of this policy are subject to college disciplinary procedures as well as local, state 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 subject to due process.

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 subject to due process.