BCCC
Baltimore City Community College

Acceptable Use of Technology Policy

Policy (check one) New__ Revised _X_Reformatted __
Applies to (check all that apply):

Faculty_X__ Staff __X__ Students_X_College _X_ All Members of the Public _X_

Topic/issue:

Standards for responsible and appropriate use of all BCCC IT and network resources for all users including BCCC students, faculty, staff, and employees under temporary contract or assignment, and campus visitors.

Policy Statement:

This policy outlines practices and constraints that a user must agree to for access to Baltimore City Community College (BCCC) IT resources.

Definitions:

IT resources include, but are not limited to, all College-owned computers, applications, software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; BCCC voice or data network traffic, including traffic entering and leaving the College network; classroom technologies; communication services and devices, including e-mail, voicemail, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems. Some College computing resources are reserved or dedicated to specific functions that may limit their use by the general BCCC community. Personal devices used to access BCCC IT resources are subject to this policy.

Acceptable Use of BCCC IT resources:

1. Understand and comply with College policies and applicable public laws. Users are responsible for understanding and complying with all laws, rules, policies, contracts, and licenses applicable to their particular uses.
2. Make reasonable efforts to protect all assigned accounts and passwords. Account owners are responsible for all actions, network use, and transactions originating from an assigned computer account.
3. Use College IT, network resources, and user accounts for appropriate College activities.
4. Respect all pertinent licenses, copyrights, and contracts.
5. Respect all restricted and/or proprietary data and information.
6. Respect the freedom, rights, and privacy of others.
7. Use IT and network resources responsibly, ethically, and with integrity.
8. Make reasonable efforts to maintain a secure home and/or personal computing environment if devices will be used to access College IT resources.

9. Acknowledge that the College may monitor computer or network use and may examine files, mail and printer history logs.
10. Report known violators of IT related College policy and/or laws to the College ITS Department.

Prohibited uses of BCCC IT resources:

1. Using another person’s BCCC IT login credentials and/or sharing your BCCC credentials with another person.
2. Misrepresenting yourself or your data on the network.
3. Transmitting threatening, harassing, intimidating, discriminatory or obscene messages.
4. Interfering with the ability of others to conduct College business.
5. Using IT resources to gain unauthorized access to or attack any remote computer or network.
6. Any intentional act that would deny or interfere with the access and use of IT resources by others, including acts that are wasteful of computing resources, or that unfairly monopolize resources to the exclusion of other users.
7. Violations of copyright law; copying, or making available on the network copyrighted material, including without limitation, software programs, music files, video files, still and digital images, radio and television broadcasts, and written text works, unless permitted by a license, by the consent of the copyright owner, by a fair use limitation under copyright law, or by permitted copying under the Digital Millennium Copyright Act (DMCA) or other law.
8. Intentional misuse or theft of software and/or IT resources.
9. Unauthorized or inappropriate access to information resources, data, equipment, or facilities, including, but not limited to tampering with components of a local-area network (LAN), or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
10. Inappropriate use of data. The unauthorized sale or transfer of data contained on College IT resources on networks (including social security number, date of birth, addresses, and other information that may be used for identity theft).
11. Unauthorized interception or monitoring of communications, user dialog, or password input, circumventing data protection schemes, exploiting security loopholes, or interfering with standard technical measures that identify and protect the rights of copyright owners.
12. Altering or disrupting system software or hardware configurations without authorization.
13. Introducing unauthorized, independent computer or network hardware to the College IT environment. Personal devices may not be connected to the College secure network without written authorization from the CIO or the CIO’s designee.
14. Unauthorized use or permitting unauthorized use of and access to electronic distribution lists and/or mailing lists created by the College.
15. Use of College IT resources for personal profit or to solicit sales for any goods, services, or contributions not authorized by the College.
16. Any other practice or use of college IT resources that is inconsistent with law, with this policy, other BCCC policies, or with the College’s mission and its role.

Violations:

Violations of this policy will be investigated and acted upon by appropriate BCCC authorities and law enforcement agencies and could result in employee discipline, sanctions, criminal prosecution, or other consequences. The College may confiscate log files, email, documents, and College-owned equipment as evidence. In its sole discretion, the College may choose to temporarily suspend or block access to an account prior to the initiation or completion of such processes, when the action is reasonable to protect the integrity, security, or functionality of IT resources, and/or to protect the College from liability.

Implementation Date: Upon Board Approval
Originator/Division: Information Technology Services
Approved by Board of Trustees: November 15, 2023