Bergen Community College
Board of Trustees
Section (IT)

Policy #: IT 005-002.2025

Effective Date: June 11, 2025

Responsible Official:
Chief Information Officer

IT Acceptable Use Policy

Policy Statement:

Bergen Community College's IT resources exist to support the academic and administrative activities needed to fulfill the college's mission. Access to these resources is a responsibility that should be exercised responsibly, ethically, and lawfully. BCC IT resources and the data residing within these systems are the property of the college and users should have no expectations of privacy while using them. Bergen Community College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Reason for Policy:

The purpose of the IT Acceptable Use Policy is to clearly communicate the responsibility each member of the college community has to protect the college's information and technology assets and to establish minimum expectations for meeting the requirements. Bergen Community College is required to be in compliance with regulations such as the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Billey Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry standards (PCI), General Data Protection Regulation (GDRP) and the Red Flag rules.

Who should read this Policy:

This policy applies to all members of the College community with access to the College network, systems and data resources, including but not limited to employees, students, alumni, volunteers, vendors, affiliated organizations, and visitors.

Definitions:

ITS: Information Technology Services

IT Resources: All tangible and intangible computing and network assets provided by the College or by ITS authorized third-parties, regardless of whether those resources or assets are accessed from on-campus or off-campus locations. Examples of such assets include, but are not limited to, hardware, software, wired and wireless network and voice telecommunications assets, mobile devices, printers and data residing on these assets.

Policy:

Acceptable use policy requires everyone to take prudent and reasonable steps to prevent unauthorized access to College systems and data. The Bergen Username forms the basis for credentials which are designed to establish ownership and responsibility for computing resources and use. Each individual should use their own user account to access BCC IT resources. Users should follow all identification and security mechanisms implemented by the college.

Using a personal device does not absolve the user from the responsibility to protect college data. Any college data on non-college-owned devices must be protected with controls equivalent to those on college-managed devices. Bergen Community College reserves the right to block unsafe devices from connecting to the network and systems. This may require users to register their device and accept terms which allow technical assessments before the device is permitted to connect. Automated device inspection utilities would block devices that do not meet security standards. Examples include outdated hardware and / or software versions, detection of malware, lack of antivirus protection, lack of a device lock-screen passcode, lack of encryption, or other security vulnerabilities.

Use of IT resources must be in accordance with College policies and codes of conduct. The ability to read, alter, or copy a file does not imply permission to do so. The College reserves the right to access and/or remove any files in violation of College policies. The ability to connect to or make use of other systems through the network does not imply the right to do so unless properly authorized by the owners of these systems. To do so without proper authorization will result in disciplinary action.

Incidental personal use is an accepted and appropriate benefit of being associated with Bergen Community College’s rich technology environment. However, this type of personal use must still adhere to all College appropriate use and related policies and procedures, and must never have an adverse impact on uses of technology and information resources in support of the College’s mission.

Bergen Community College reserves the right to immediately take any action it deems necessary, including but not limited to disconnection and quarantine of devices and/or

suspension of user accounts or services, to maintain the stability, security and operational effectiveness of computing and network resources.

Prohibited Activities:

College information technology resources may not be used in any manner prohibited by state and federal laws or disallowed by licenses, contracts or policy. This section, while not all-inclusive, lists examples of misuse that would constitute a violation of this policy.

Individuals using BCC's IT Resources are not permitted to:

- Install non-college-related software or downloads on college-provided computers, without the permission of Information Technology Services (ITS).
- Use BCC IT Resources for the purpose of advertising or running an organization or business not affiliated with the College or for personal gain.
- Send, view and/or print lewd or pornographic materials for non-academic purposes.
- Reveal their password to anyone including employees, or let another person use their BCC account. Likewise, users should not use anyone else's credentials for any college systems or services. Each user is responsible for what is done with their BCC account.
- Share codes or approve multi-factor authentication (MFA) prompts unless they are for their own login.
- Use passwords that are weak or can be easily guessed. Users are responsible for establishing unique passwords that comply with BCC password standards including length and complexity requirements. Users must protect their passwords from disclosure and should not record or store them insecurely.
- Use personal accounts to conduct college business.
- Use the same password for BCC and non-BCC or personal accounts.
- Engage in intentional malicious activity designed to harm systems, computers and networks. Such activity includes but is not limited to: hacking systems; disabling or crashing systems; network sniffing; sending viruses, malware or mass email; creating unnecessary or multiple jobs and processes.
- Take BCC IT Resources such as Desktop Computers, monitors, printers, scanners, webcams, etc. off-site without prior authorization from ITS.

- Failure to follow college data handling requirements for restricted information (Information classified as ‘Private’ and ‘Confidential’ in the college’s Data Classification policy). Examples include but are not limited to:
    - Accessing or processing restricted college information over public insecure networks. Instead, use an approved secure connection method such as VDI.
    - Storing restricted college information on non-college computers or removable media (phones, tablets, USB drives, etc.), which is prohibited. Any portable device storing confidential college information must be encrypted, and must be securely transported and stored when not in use. Laptops issued by the college to BCC employees are encrypted.
    - Storing, transmitting or sharing restricted college data using solutions not approved and securely managed by ITS. Restricted data should not be stored or shared using non-BCC-provided methods or tools, such as peer to peer sharing, Dropbox, etc.
    - Transmitting restricted college information by email to distribution lists. Emails containing restricted data should always be protected using the BCC approved encryption technology.

- Bypass security mechanisms, circumvent data-protection or system consistency schemes, force unauthorized access, or attempt to exploit security loopholes.

- Leave a computer or device unattended without locking the screen to prevent unauthorized access to college systems or information. Any device used to access college systems or data must have a lock screen enabled.

- Install, attach, connect, remove or disconnect computing or network hardware to college information systems without approval from ITS.

- Send harassing, obscene, libelous, or threatening messages.

- Aid or abet another person in violating any part of this Policy, or prevent anyone from reporting an incident.

- Violate any other state, local or federal laws or regulations pertaining to cyber security.

Enforcement:

This policy is intended to comply with and augment the BCC Student/Employee Code of Conduct and all local, state, and federal laws. Individuals who violate any part of the policy will be subject to college disciplinary action (in accordance with all applicable collective bargaining

agreements). Access to select or all BCC IT Resources may be revoked during the investigation of an alleged violation, or a finding of violation of this policy.

Incident Reporting:

In order to detect and respond promptly to security incidents and limit the harm to the college, users have a responsibility to immediately report to the BCC Help Desk the loss, theft, inappropriate use, suspicious activity and/or other signs of compromised systems, data, access credentials, security tokens, or devices.

Related Documents/Policies:

- Data Classification and Handling Policy
- BCC Google Drive Docs Usage Guidelines and Support Agreement

Policy History (adopted/amended):

Adopted: June 10, 2025
Amended: