

BRTC Campus Computer and Network Acceptable Use Policy

Purpose

The computing resources at Black River Technical College support the educational, instructional, research, and administrative activities of the College and the use of these resources is a privilege that is extended to members of the BRTC community. As a user of these services and facilities, you have access to valuable College resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the College can take disciplinary action, including the restriction and possible loss of network privileges. Violation could result in more serious consequences up to and including suspension or termination from the College. Individuals are also subject to federal, state and local laws and regulations governing computer and network use as well as interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

This document establishes specific requirements for the use of all computing and network resources at BRTC and applies to all users of computing resources owned or managed by BRTC.

Acceptable Use

- 1) You may use only the computers, computer accounts, and computer files for which you have authorization.
- 2) You may not use another individual's account or attempt to capture or guess other users' passwords.
- 3) You are individually responsible for appropriate use of your computer, account and all resources assigned to you.
- 4) The college is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- 5) You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access.
- 6) You must not attempt to access restricted portions of the network, individual computers, or attempt to monitor network traffic without approval of Computer Services.
- 7) You must not develop or use programs, software, or processes that disrupt other computer or network users, or that damage or degrade performance, software, or hardware components of a system.

Unacceptable Use

1. Users may not use the campus computing or network services to transmit or display information which
 - a. Violates or infringes on the rights of another person, including the right of privacy.
 - b. Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
 - c. Violates BRTC policy prohibiting sexual harassment.
 - d. Restricts or inhibits other users from using the system or the efficiency of the computer systems.
 - e. Uses the system for any illegal purpose.
2. Users may not illegally share or obtain copyrighted material
3. Users may not use computing and network services for uses that are inconsistent, incompatible, or in conflict with state or federal law or BRTC policy.
4. Users must respect the privacy of other users, including others digital property.
5. Users may not share their password with others or let others use their account .
6. Users must respect the intellectual property of others and adhere to College standards of academic honesty.
7. Users must not intentionally disrupt the campus computing system or obstruct the work of other users such as by interfering with the accounts of others, introducing or spreading viruses or other destructive programs on computers or the network, sending chain letters or blanket e-mail messages, or knowingly consuming inordinately large amounts of system resources.

Computer Labs

The primary purpose of the computer labs is to allow BRTC students a place for computer-based learning and research. As such, the following guidelines should be followed while in the computer labs:

- 1) Be considerate of other users. The labs are intended to be places of study and academic work and every effort is made to maintain this environment. If conversation is necessary for your work, please do so quietly. Acceptable noise volume levels will be at the discretion of the computer lab assistant or instructor on duty.
- 2) Cell phone conversations are prohibited in the labs. Please use cell phones outside the lab.
- 3) Music or other audio should not be audible to other patrons or the lab assistant. Please use headphones in the labs. If others can still hear your audio content, you will be asked to turn the volume down.
- 4) Children are not allowed unless accompanied by an adult. If they disturb others, you will be asked to leave. Your children are not to be left unattended anywhere on campus. Please be aware that computers in the labs have full access to the Internet and there are no content

filters to prevent children from accessing or viewing inappropriate materials.

- 5) No food or drink in labs.
- 6) Password sharing and logging in for other users is prohibited.
- 7) Students are not allowed to install software or otherwise tamper with the hardware or software of the lab computers.
- 8) Printing in the computer labs will be limited per student account. Access to and volume of printing is also at the discretion of the lab assistant or instructor.
- 9) Accessibility stations are reserved for users with special requirements. You may use one if it is available, but you will be asked to relocate if a user with special needs is present.
- 10) Playing games, chatting, social networking and other recreational use of lab computers is not to get in the way of students needing to do academic work. During periods of peak usage, users doing non-academic work may be asked to give up their workstation for a user who needs to do academic work.
- 11) Please do not leave personal belongings in the lab for any length of time. We are not responsible for missing items.
- 12) Dispose of any trash in the waste receptacles provided.
- 13) Comply with all requests and instructions from the lab assistant. Should you have an issue with any request being made of you, please request to speak to a supervisor.

Wireless Access

BRTC provides wireless network access on the Pocahontas and Paragould campuses for internet use only. Use of these WiFi networks are covered by this computer use policy and acceptance of this is required for access.

Public Access

BRTC provides public access computing in designated areas only. Use of these public computers is subject to this computer use policy and all public users must comply with all requests and instructions from the lab assistant.

Student Accounts and Data

Student accounts (lab use and email accounts) are created at the beginning of each semester for all currently enrolled students. All student accounts and stored data are deleted before each fall semester. Student email accounts are deleted after two consecutive semesters of non-enrollment or at the request of the student. Students are encouraged to backup important data to flash drives.

BRTC Campus Computer and Network Acceptable Use Policy

Faculty and Staff Only

Wireless Access to Student Information System

Due to security concerns, accessing the Student Information System (POISE) using SmartTerm or other terminal emulation software is prohibited when using wireless network access. If temporary wireless access is required then only SSH connections should be used. This does not apply to normal browser-based access (CampusConnect). Please contact Computer Services for assistance if you have any questions.

Remote Access and VPN

Remote access and Virtual Private Network (VPN) services allows computers to connect to the BRTC data network from off-campus, thereby potentially granting those computers the same access, rights, and privileges as computers attached to the campus network directly. This policy governs appropriate use of remote access and VPN by all employees and third party workers.

Users and machines connected remotely must abide by all policies of the College including, but not limited to, the BRTC Campus Computer and Network Acceptable Use Policy.

Additionally:

- It is the responsibility of users with remote access/VPN privileges to ensure that unauthorized users are not allowed access to BRTC's internal networks.
- All computers that access campus resources via remote access/VPN must adhere to any guidelines set by the College.
- It is the responsibility of supervisors and department heads to:
 - determine which of their office/department's college business activities can and cannot be performed via remote access/VPN from off-campus;
 - determine under what circumstances it is appropriate for an employee to use remote access/VPN to conduct college business, and to request the approval of the Human Resources Office when necessary;
 - communicate the above to their employees.
- Only remote access/VPN clients and users approved by Computer Services will be authorized to connect via VPN.
- It is the responsibility of all remote access/VPN users to keep secure all files, keys, and passwords required to connect via remote access/VPN.

BRTC Campus Computer and Network Acceptable Use Policy

Faculty and Staff Only

By signing this form you are acknowledging that you have read, understand, and agree to comply with the above principles governing the use of BRTC technology resources.

Date _____

Name (please print) _____

Department _____

Signature _____

Contact number _____

[Dated 4/10/2015]