BROWN MACKIE COLLEGE

Technology & Computer Lab Handbook

Introduction

1.1 Welcome to Brown Mackie College! We encourage you to use the computer labs while studying here. The campus technology team is here to provide access to hardware and software and to administer all technology resources through policy guidelines. Our goal is to provide fair and efficient service to all students and faculty.

1.2 Use this guide and familiarize yourself with the policies and procedures regarding using technology resources available to you on campus and online. Our intention with this handbook is to provide clear direction on matters that come up frequently.

Computer Lab Policies

2.1 Users must respect others' privacy, including text (electronic mail and file transfer) and images (graphics and video).

2.2 No cell phones may be used by faculty or students in the computer labs as a courtesy to others using the labs. Cell phones must be turned off prior to entering the labs.

2.3 No eating, drinking, or tobacco use of any kind is permitted in the computer labs. Open containers are not allowed on carpeted areas or outside the lab entrance.

2.4 Open labs are designed for completion of College work only. Use of College computer labs for playing games is prohibited.

2.5 No student peripherals or software may be used or installed in College computer labs without expressed written consent from the Technology Support Supervisor.

2.6 During open lab times, leave the computers with specific uses open for student access. These include computers with dedicated scanners or video equipment.

2.7 The College is not responsible for your data. Please utilize removable storage where available or email important files to yourself to maintain a backup of any important documents that you create.

2.8 Using the network for illegal file sharing, music sharing, and otherwise illegal downloading of any copyrighted material is not allowed. Violation of this policy will result in disciplinary action and/or legal action.

2.9 It is inappropriate to violate software license agreements by making unauthorized copies of computer software or loading unauthorized copies of software onto the College's computers.

2.10 It is inappropriate to send e-mail messages that include profanity, vulgarity, or discriminatory or derogatory language or remarks.

2.11 It is inappropriate to broadcast messages of personal statements regarding private issues, especially those of a political, religious, or controversial nature.

2.12 It is inappropriate to use facilities for soliciting other students, sending chain letters, or for pranks.

2.13 It is inappropriate to use Web access to visit sites that are pornographic, vulgar, obscene, or that are otherwise of questionable moral value. In addition, sites that contain illegal information or images (child pornography, etc) should never be accessed for any reason. Violation of this policy will result in disciplinary action and/or legal action.

2.14 It is inappropriate to use facilities for illegal activities.

2.15 Do not modify the system environment in any way. This includes changes to the screen backgrounds, screen savers, or disconnect the computer system hardware.

2.16 Personal storage devices should be checked with virus protection software regularly to help prevent infection.

2.17 When using the computers for audio or video playback, please use headphones so as not to disturb others in the lab.

2.18 It is in appropriate to use the computing facilities to interfere with normal operations of the school network or computer systems.

These rules and policies exist to make the labs effective for all users. Failure to comply with lab policies may result in your being asked to leave the lab, either for the day, or in the case of repeat or egregious offenses, for longer.

Computer Lab Hours

3.1 Instructional Computer Labs at our campus have Open Lab hours when the lab is not being utilized for class. To determine which labs are available for general open lab use, please consult the lab schedule posted outside each computer lab. Lab hours change monthly. Students are required to exit an open lab fifteen minutes prior to the start of any classes to allow students in the next class to setup and prepare for class activities.

3.2 Our campus has a computer lab located in our Learning Resource Center. This lab can be used to do online research, homework, and for general computer use. You can access this computer lab whenever the Library is open.

Using the College Network

4.1 Students logging into the Citrix student desktop environment automatically have access to a personal storage area on our college file server. This personal storage is called your 'Home' drive and is mapped with the letter 'H:/'. Use this space to store work in progress during classes and make regular backups of this data by emailing the files to yourself or by uploading them to a 3rd party service such as Microsoft SkyDrive or an FTP server location of your choice.

4.2 All Labs have access to the Public, Shared, or Instructor file server shares. We have a very comprehensive computer network. This lets staff, faculty, and students move large files from lab to lab easily. The purpose of the file server is to allow temporary movement of files from the lab to another location. Do not store files on the server shares in place of your own backup storage. Faculty may have you place assignments, project files, or other media on the server for others to view, but the files should still be considered temporary while on the server.

4.3 Do not erase files from the server other than your own. Place files only in a folder labeled with your last name. Please delete your individual files from the server once you have moved them to your personal storage device or electronically transferred them to your own personal storage space via email or FTP.

Problem Reporting

5.1 Despite the quality of the equipment and your careful use, sometimes computers do malfunction. It is the same here at Brown Mackie College as anyplace else you will ever go to work or school. One reason problems occur is that the machines are simply used by so many different people. The machines are truly not personal computers, but are used by hundreds of users per month. With this in mind, help us to track and repair problems quickly by opening a technology 'trouble ticket' available at http://bmcsupport.brownmackie.edu. This ticket is essential and only takes a few seconds to fill out. Once we address the issue, we will notify you via email the problem is resolved and you can close the open trouble ticket confirming for us that the computer is working properly again.

5.2 Troubleshooting -- Over 90% of reported problems can be fixed simply by returning the machine to its default state by rebooting it and logging back in. We run special software that returns a computer to a standard setting each time it restarts.

Printing

6.1 Each lab has a black and white laser printer. The printers are set-up so that you can print to any printer on campus through the network. Please double-check that you are connected to the printer in your lab prior to sending prints to the queue. Please limit black and white prints to no more than a few pages and not more than one copy. If you need additional copies, print one master and then use the copier in the Library. Since use of these printers are free of charge, please do not use the printers for non-school work. If the printers need toner or paper please alert a faculty or staff member so that it can be refilled. If the printer gets jammed, please do not attempt to remove the jammed paper yourself. Allow a faculty or staff member to assist with any printer related issues. Only standard laser paper should be used with lab printers.

Internet & Network Usage Policy

7.1 Policy for the Responsible Use of Information Technology at Brown Mackie College. Preamble - In support of its mission, Brown Mackie College provides access to information resources for students, faculty, and staff within institutional priorities and financial capabilities.

7.2 The Policy for Responsible Use of Information Technology at Brown Mackie College contains the governing philosophy for regulating faculty, student, and staff use of Brown Mackie College's information technology resources. It spells out the general principles regarding the appropriate use of equipment, software, network, and Internet. By adopting this policy, Brown Mackie College recognizes that, all members of Brown Mackie College are bound by local, state, and federal laws relating to copyrights, security, and other statutes regarding electronic media and data transmission. The policy also recognizes the responsibility of faculty and system administrators to take a leadership role in implementing the policy and assuring that the Brown Mackie College community complies with the policy.

7.3 All members of the Brown Mackie College community who use the Brown Mackie College computing, information, and communication resources must act responsibly. Every user is responsible for the integrity of these resources under their control. All users of BMC-owned or BMC-leased information technology systems must respect the rights of other users, respect the integrity of the physical facilities and controls, and comply with all pertinent licenses and contractual obligations, and the highest standard of ethics.

7.4 Information technology provides important means of communication, both public and private. Users and system administrators will respect the privacy of person-to-person communication in all forms, including voice (telephone), text (electronic mail and file transfer), and image (graphics and video). The principle of freedom of speech will apply to public communications in all these forms, but students and staff who are provided access to Brown Mackie

College computer facilities and to the network and World Wide Web assume responsibility for their appropriate use. BMC expects students to be careful, honest, responsible, and civil in the use of computers and networks.

7.5 Computer systems and networks provide mechanisms for the protection of private information from unauthorized access, and these mechanisms are necessarily imperfect and any attempt to circumvent them in order to gain unauthorized access to such data will be treated as a violation of privacy, and will make a student eligible for disciplinary action. In open access use of Intranet and Internet communications, students are individually responsible for ethical, aesthetic and purposeful use that directly contributes to the academic environment. We will not and cannot define here limits and boundaries for unethical use, such as access to vulgar, illegal, or material of a questionable moral or otherwise redeeming value. It is the policy of Brown Mackie College for students, faculty and staff to maintain such high standards in these matters that no question will arise as to unacceptable conduct or computer misuse. Reports or discovery of suspected abuse will be immediately investigated, and disciplinary action indicated in this document including exclusion from use of the computing facilities will be administered as deemed in the best interest of the BMC community.

7.6 Access to Brown Mackie College information technology facilities is a privilege granted to BMC students, faculty, and staff. Access to BMC information resources may be granted based on the following factors: relevant laws and contractual obligations, the requester's need to know, the information's sensitivity and the risk of damage to or loss by BMC.

7.7 Brown Mackie College reserves the right to extend, limit, restrict, or deny privileges and access to its information resources. No individuals other than BMC faculty, staff, and students may be permitted access to BMC computers, without the express written consent of the Campus President or Dean of Academic Affairs. In such event, access is allowed to the extent that information access does not violate any license or contractual agreement; BMC policy; or any federal, state, county, or local law or ordinance.

7.8 BMC facilities and accounts are to be used for the activities or purposes for which they are assigned. Brown Mackie College computing resources are not to be used for commercial purposes without written authorization from Brown Mackie College In these cases, BMC will require payment of appropriate fees. This policy applies equally to all Brown Mackie College owned or leased equipment.

7.9 Users and system administrators must all guard against abuses that disrupt or threaten the viability of all systems, including those at Brown Mackie College and those on networks to which BMC's systems are connected. Access to information resources without proper authorization from the data owner, unauthorized use of BMC facilities, and intentional corruption or misuse of information resources are direct violations of BMC's standards for conduct, and may also bring civil or criminal charges against the offenders.

7.10 The Regional Director of Technology is responsible for adopting guidelines for the implementation of this policy. Local staff and central staff system administrators may adopt additional guidelines for the use of their own systems and are responsible for making the policy and guidelines available to all users. To this end the Web Master and Network Administrators have limited access to websites that have been deemed as a security risk, contains material of a questionable nature, or provides a risk to the stability of the network.

7.11 Alleged violations of this policy shall be subject to the procedures outlined in the Brown Mackie College student handbook. Brown Mackie College treats access and use violations of computing facilities, equipment, software, information resources, networks, or privileges seriously. Brown Mackie College will pursue criminal and civil prosecution of violators when appropriate.

7.12 The guidelines above are not meant to be exhaustive, and in exceptional circumstances, they may yield. Their enumeration here is intended to emphasize the importance of approaching these issues in a sensible, professional way consistent with the accepted principles of the academic community and orderly and efficient workplace. The judgment and discretion of BMC staff -- guided, when appropriate, by legal counsel -- will continue to be the foundation on which responsible decisions are grounded.

Wireless Access

8.1 Brown Mackie College makes available a wireless network for student use. This wireless network is secured using an application called Cisco Clean Access. When connecting to the wireless network, you will be prompted to install a small applet on your computer and it will check your computer to ensure you have appropriate virus protection before allowing you onto the Internet.

8.2 When connecting to the wireless system, please choose the STUDENT_WIFI ssid and launch your Internet browser to begin. You will need to have your student portal username and password to connect to the wireless network.

8.3 Use of the wireless network is at your own risk. The College is not responsible for virus infections or other malware that may end up on your computer as a result of using the wireless system. It is highly recommended that students using the wireless network have up to date virus protection and have downloaded and installed the latest operating system updates from Microsoft (Windows) or Apple (Mac OS X).

8.4 All acceptable use policies described in this handbook also apply to the wireless network.

Privacy and Security Awareness Bulletin

Dear Students,

Identity theft is a significant national problem. Identity theft occurs when someone uses your personal information in an effort to commit fraud or for another unlawful purpose. Once an identity thief has your personal information, he or she could open new credit card accounts in your name, take out a loan in your name, or engage in other fraudulent activities in your name. If you are a victim of identity theft, restoring your credit and dealing with identity theft can be a slow, time-consuming and costly process.

Identity thieves try to steal the personal information they need from many sources, including directly from their victims. We want to provide you with some tips to help you protect your personal information:

- Identity thieves need personal information about you to commit their crimes. Safeguard the types of information that can be most helpful to them in efforts to set up fraudulent accounts in your name or take over existing accounts that you have. Examples include your:
    - Social Security number;
    - Driver's License number;
    - Date of Birth;
    - Other government identification numbers such as your passport, state issued identification card numbers, tribal identification card numbers, etc.;
    - Financial account numbers (checking, savings, debit card, credit card, etc.) as well as any personal identification numbers, codes, or passwords necessary to access those accounts, such as your mother's maiden name; and
    - User IDs and passwords for your e-mail, social media, financial, and other accounts.

  We ask that you never send us (or anyone else) this information through email.

- When using mobile devices, keep some tips in mind to help keep your information and device safe:
    - Always secure it (and any online accounts you have) with strong password that is easy to remember and hard to guess. Use a phrase in a song that you like with upper and lower case letters, numbers and special characters.
    - Set up any tracking and remote wiping functionality that comes with your device.
    - Be cautious of the applications you download. Download apps only from trustworthy sources.
    - Don't "root" or "jailbreak" your device or install third-party firmware.
    - Never leave your device unattended.

- It is not only electronic information that is of potential value to identity thieves. Safeguard your physical driver's license and other identification documents, credit cards and statements, as well as your bank account statements, tax returns and any other documents that have sensitive personal information. These things should be shredded when they are no longer needed.

- Be skeptical of online requests to provide your personal information. Identity thieves often try to send e-mails designed to impersonate schools, banks, and other institutions that you have relationships with in order to trick you into providing personal information or clicking on a link that can allow the thieves to infect your electronic devices and steal information from your device. Do not click links from unknown sources as it may give them a way in to create a virus on your computer and never click a link that asks for sensitive info.

If you have any questions or need any assistance, contact the Support Center at 1-866-847-8848 or email campus_support@brownmackie.edu.