CP 1.22.1
Acceptable Use of Computer Resources, Internet and Network

Related Board of Trustee Policy: BP 1.22

Responsible Official	*Director of Technology and Information Services*
Approvals	*01/10/08*
Revision	*06/27/2023*
	07/12/2023
	08/04/2023
	09/06/2023
	09/13/2023

Procedure

Definitions

Administrative Officer: Vice-President, Dean, or Director to whom an individual reports.

Computer Account: The combination of a user number, user name, or user I.D., and a password that allows an individual access to a mainframe computer or some other shared computer or network.

Information Resources: Data or information as well as the software and/or hardware that make the data or information available to users.

Network: A group of computers and peripherals that share information electronically, typically connected to each other by either a cable or satellite link.

Servers: "Central" computers capable of use by several people at once.

Software: Programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, or optical media (CDs, DVDs), etc.), usually used to refer to computer programs.

System Administrator: Staff employed by a central computing agency such as the Technology Department whose responsibilities include system, site, or network administration and staff.

System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. If a person has a computer on his/her desk, he/she may be acting, in whole or in part, as that system's system administrator.

User: Anyone who does not have system administrator responsibilities for a computer system or network but who makes use of that computer system or network. A user is responsible for his/her use of the computer and for learning proper data management strategies.

Computer: Personal computer, laptop, servers, or any other device that utilizes an operating system.

I.T. Resource: Any software, data, equipment, purchased and maintained by McDowell Technical Community College.

Network Devices: Includes printers, copiers, scanners, facsimile machine, telephones, switches, routers, Access Points, hubs, or other electronic devices designed to work or manipulate or monitor network systems.

Responsible Administrative Computing

The following rules and prohibitions define acceptable use of the college computing systems whose primary users are faculty and staff using the system for college business (i.e. the computing system in the Technology Department). Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as disciplinary or legal sanctions under federal, state, or local law.

All users of this system must comply with the principles outlined in this procedure. By using this system, users agree that they understand and will comply with these principles:

1. The college owns the system. All information contained on the system is college property. The college reserves all rights to the system, including termination of service without notice. Users of this system have rights that may be protected by federal, state, and local law.

2. Computer facilities and accounts are owned by the college and are to be used for college-related activities only. College computing resources are not to be used for commercial purposes or non-college related activities without written authorization from the college. Written authorization must come through the Director of Technology and Information Systems and then through the President's office for final approval. All access to central computer systems, including the issuance of passwords, must be approved through the office of Director of Technology and Information Systems.

3. Each faculty/staff member is responsible for maintaining access control for his/her assigned computer equipment in an effort to keep equipment and shared data secure. Users who do not have a computer account assigned to them must see the Director of Technology and Information Systems to initiate the proper documentation (*Datatel User Request Form or IT Systems Access Request Form*) for obtaining an account. Use of someone else's user account and/or password is not acceptable. Doing this could be considered falsification of information. The individual is responsible for the proper use of the account, including proper password protection. Users should change their password regularly. Report unauthorized use of accounts to the Project Director, Supervisor, System Administrator or other appropriate college administrative officer. Also, users must log out of programs when not using their computer or when the user will be away from his/her desk for more than five (5) minutes.

4. Programs and files are confidential unless they have explicitly been made available to other authorized individuals. The college reserves the right to access all information stored on college computers. File owners will be notified, in advance, if such notice is practical. When performing maintenance, every effort is made to ensure the privacy of a user's files. However, if violations are discovered, they should be reported immediately to the appropriate administrative officer.

5. Electronic communications facilities (such as EMAIL) are for college-related activities only. The college supports the State's policy on the use of college owned and the state operated network.

6. The college provides virus scanning software that should be used by all computers within the college. Users that bring data to the college computers must scan the media before using it on any computer. The college supported anti-virus software must not be disabled or tampered with by the end users.

All users of this system must comply with the prohibitions outlined in this procedure. By using this system, users agree that they understand and will comply with these prohibitions:

1. Wastefully using finite resources, such as large amounts of bandwidth for an extended period of time.

2. Using chat rooms or instant messaging, other than in support of the research, educational, and administrative purposes of the College.

3. Sending fraudulent computer mail, breaking into another user's electronic mailbox, or reading someone else's electronic mail without his or her permission are some, but not all, actions that can be characterized as misuse of the computing resources.

4. Individuals may not conduct activities for personal gain. This includes advertising personal services, selling, soliciting jobs, or any other activities whose purpose is to generate revenue for an organization or for the individual's personal gain.

5. Using, distributing, or making accessible profane, obscene, pornographic, or discriminatory images or remarks, or other content which reasonably may be considered to be offensive to another user; or participating in other antisocial behavior.

6. Disclosing student information in violation of the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA).

7. No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any college computer system. This includes, but is not limited to, deliberately downloading, uploading, creating, or transmitting computer viruses.

8. Destroying or modifying directory structures or registries; or interfering or tampering with another's data or files.

9. Using computer resources for political campaigns or distribution of political material.

10. Developing programs that infiltrate a computer or computing system, harass other users, and/or damage software.

11. Computer software protected by copyright is not to be copied from, into, or by using campus computing facilities except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied to make backup copies, if permitted by the copyright owner. The number of copies and distribution may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

12. Users are not authorized to install new software, or updates to existing software on the college-owned computers. All desktop and laptop computers are configured in standard formats for administrative and instructional users. These configurations are developed and tested by the Technology Department. If a user needs additional software installed on their office computer or in a computer classroom, they should contact the Director of Technology and Information Systems for this purpose. Users should not install copies of personally owned software on college desktop computers or laptops. No software should be installed from outside sources due to licensing issues and liabilities. Outside sources include, but are not limited to; screen savers, wall paper, games or programs that are readily available on the Internet. Unauthorized software found on college computers will be removed by the Technology Department staff.

13. Users are not authorized to connect personally owned computers or laptops to the college network without prior approval from their supervisor and the Director of Technology and Information Systems. The user will be required to allow Technology Department staff to install appropriate anti-virus software and client/server software on the computer or laptop before it is connected to the network. If the computer or laptop is not using an operating system that is compatible with the standard anti-virus software provided by the college, or the client/server software, the software will not be installed and access will be denied.

    The college uses several methods to protect the computer systems and critical information within the wide-area network operated by the college. A firewall server protects the internal network by limiting access from external sources to only the servers intended for public access, the college web server and the online courses server. The internal network has been further subdivided into VLAN's (Virtual Local Area Networks) that isolate traffic by port and end user. The college installs anti-virus software on all desktop and laptop computers along with client/server software. The client/server software provides a method of regularly updating the anti-virus definitions.

    If an unauthorized computer or laptop is connected to the internal network, there is a possibility that a program or virus will be introduced that will disrupt the function of the network and/or the authorized computers connected to the network. Users that violate this policy may be held accountable for the expenses caused by such a disruption.

14. Work-study students will not be assigned to the following areas, due to the confidential nature of business conducted on a routine basis: Human Resources, Payroll/Cashier/Business Office, and other designated departments/offices. Work-study students are prohibited from engaging in any operational functions that include access to confidential files, academic and personnel records, or other related materials and information resources. The college reserves the right to grant work-study students temporary access to Datatel; any exceptions made in this regard will be extremely rare.

Responsible Instructional Computing

The following rules and prohibitions define acceptable use of all college computing systems whose primary users are faculty, staff, students, and other authorized individuals. The instructional computing systems are to be used to support the educational programs of the college and are to be used for such related activities only. College computing resources are not to be used for commercial purposes or non-college related activities. Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as, prosecution under federal, state, and local law.

All users of the college's instructional computing systems must comply with the procedures outlined in this document. By using any of these systems, users agree that they will comply with these procedures or prohibitions.

1. The college reserves all rights, including termination of services without notice, to the instructional computing resources that it owns and operates. Users of these systems have rights that may need to be protected by federal, state and local law.
2. Access and privileges to the college instructional computing systems are assigned and managed by the system administrators of specific individual systems.
3. User Responsibilities:
    A. Maintain an environment in which resources are shared equitably between users.
    B. Maintain an environment that is conducive to learning.

- A user, who harasses or makes defamatory remarks, shall bear full responsibility for his or her actions. Further, by using the system, users agree that individuals who transmit such remarks shall bear sole responsibility for his or her actions. User agree that the college's role in managing this system is only as an information carrier, and that he or she will never consider transmission through this system as an endorsement of said transmission by the college.
- Many of the college's instructional computing systems provide access to outside networks both public and private which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that the college does not assume responsibility for the contents of any of these outside networks. The user agrees to comply with the acceptable use guidelines for any outside networks or services he/she may access through the college systems. Further, the user agrees to follow proper etiquette on outside networks as defined by that network.
- The user agrees never to attempt to transmit, or cause to be transmitted, any messages in which the origination is deliberately misleading. The user agrees never to attempt to transmit, or cause to be transmitted, any message that is inconsistent with an environment conducive to learning or with a misleading origination. The person who performed the transmission will be solely accountable for the message, not the college, which is acting solely as the information carrier.
- The user shall not us the system in such a manner as to disrupt the business of the college by creating, displaying, transmitting, receiving or making accessible threatening, racist, sexist, obscene, offensive, annoying or harassing language and/or material, including broadcasting unsolicited messages or sending unwanted mail or otherwise.

C. Maintain a secure environment.

- Knowledge of passwords or loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.
- Users are responsible for proper password maintenance, including periodic changes and safeguarding the password.
- Users are responsible for backing up their own data.

4. Computer software protected by copyright shall not be copied from, into, of by means of college computing facilities, except as permitted by law or by the contract with the owner of the copyright. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users exceeds the number of original copies purchased.
5. Violating copyright laws and/or fair use provision by downloading or uploading pirated or illegal material, including, but not limited to, software and music files; inappropriately reproducing or disseminating Internet material, except as permitted by law or by written agreement with the owner of the copyright.
6. Attempting to obtain unauthorized computer access or privileges, or attempting to trespass in the work of another individual.

7. Using hardware or software sniffers to examine network traffic, except by appropriate College personnel to diagnose the network for bottlenecks or other problems.
8. Committing any form of vandalism on equipment, communications lines, manual, or software; attempting to defeat or circumvent any security measures or controls.
9. Consuming food and/or beverages in computer labs, computer classrooms, or in any other areas restricted to protect systems.
10. Using a bootable CD/Device to temporarily or permanently alter McDowell Technical Community College computer system outside of their intended configuration.
11. Connecting unsanctioned products (software or hardware) to the College network, or installing products for personal use. Special provision may be made for visiting trainers at the discretion of the Director of Technology and Information Systems. TIS support can offer assistance in gaining network access under these special circumstances, but the College cannot guarantee functionality, and assumes no responsibility for configuration of or damage to Non-College equipment.

Reservation of Rights and Limits of Liability

1. McDowell Technical Community College reserves all rights in the use and operation of its computer resources, including the right to monitor and inspect computerized files or to terminate service at any time and for any reason without notice.

2. The College makes no guarantees or representations, either explicit or implied, that user files and/or accounts are private and secure. No right of privacy exists in regard to email or internet sessions.

3. The college is not responsible for the accuracy, content, or quality of information obtained through or stored on the College network.

4. The College and its representatives are not liable for any damages and/or losses associated with the use of any of its computer resources or services.

5. The College reserves the right to limit the allocation of computer resources.

6. The College makes efforts to maintain computer resources in good working condition but is not liable for damages incurred by loss of service.
7. College funds may not be used to purchase personal network access or products.

8. The College is not liable, legally, financially, or otherwise, for the actions of anyone connecting to the Internet through College systems.

Electronic Mail

College computer resources may be used to access electronic mail systems and resources. The use of College resources for electronic mail must be related to College business, including academic pursuits. Incident and occasional personal use of electronic mail is acceptable when such use does not generate a direct cost to the College. The College will make reasonable efforts to maintain the integrity and effective operation of its electronic mail system, but users are advised that this system should in no way be regarded as a secure medium for the communication of sensitive or confidential information.

Electronic Mail (email) is Property of the College. Because of the nature and technology of electronic communication, the College can assure neither privacy of an individual's use of the College's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored. Any email correspondence generated or received by an MTCC computer is the property of the

College and is subject to the North Carolina Public Records Law and may be disclosed to third parties (Ref. NC G.S. c. 132). The College does not monitor electronic mail as a routine matter, but may do so to the extent permitted by law, as the College deems necessary. Any user of the College's computer resources who makes us of an encryption device shall provide access when requested to do so by the appropriate College authority. The College reserves the right to access and disclose the contents of employee's electronic mail without the consent of the user. The College will do so when it believes it has a legitimate business need including but not limited to those listed below.

1. In the course of an investigation triggered by indications of misconduct or misuse.

2. As needed to protect health and safety.

3. As needed to prevent interference with the academic mission.
4. As needed to locate substantive information required for College business that is not more readily available.

5. As needed to respond to legal actions.

6. As needed to fulfill the College's obligation to third parties.

All email users must respect the following rules:

1. All messages received or sent over MTCC computing resources, systems, or networks should correctly identify the creator and receiver of such.

2. The college reserves the right to access and disclose all messages including the right to disclose to law enforcement officials.

3. The use of electronic mail for commercial or private business purposes is prohibited.

4. No received or transmitted message shall be permitted to overload the College's compute systems, be harmful, or have a negative impact on the system's performance.

5. Sending junk mail, spam, or other advertising material is prohibited.

6. The creating or forwarding of "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.

7. The College is neither responsible for any archival storage, nor retained email messages.

8. Transmitting or making accessible threatening, racist, obscene, offensive, annoying or harassing language and/or material is prohibited.

Electronic mail may constitute "education records" as defined in the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). Electronic mail that meets the definition of education records is subject to the provisions of FERPA. The College may access, inspect, and disclose such records under conditions set forth in the federal statute.

North Carolina law provides that communications of College personnel that are sent by electronic mail may constitute "correspondence" and, therefore, may be considered public records subject to public inspection under the North Carolina General Statutes, chapters 121 and 132.

Electronic files, including electronic mail, that are considered to be public records are to be retained, archived and/or disposed of in accordance with current guidelines established by the North Carolina Department of Cultural Resources.

Other Responsible Computing Procedures

Computer Backup

Software and data on the central computers systems are maintained by the Director of Technology / Information Systems. Full back-ups are performed on a daily basis.

Data maintained electronically on a computer system is always at risk to some degree. At risk factors are minimized as much as possible through backup, and maintenance / security procedures; however, the possibility still exists (however remote) for loss of data in spite of best efforts. Users should be aware of this situation and maintain printed copies of important reports and all non-replaceable source documents. General current audit guidelines require sufficient printed documentation to reconstruct data if disaster strikes.

Faculty / staff members using microcomputer equipment must be completely responsible for their own data maintenance and backup procedures. Microcomputer users should be aware of the fact that electronically sorted data is extremely sensitive and can readily become irretrievable. The only defense is to maintain numerous current backups and printed file copies of vital information in case disaster strikes.

Computer and Technology Support

Maintenance of computers, networks, most communications equipment, and related software is the responsibility of the Technology Department through it's Help Desk. Such service may include:

1. Installation of computer hardware and software.
2. Writing specifications for new equipment.
3. Initiating requisitions for new equipment.
4. New account and account change requests.
5. Hardware repair and upgrades.
6. Telephone system support.
7. System printing requests.
8. Technology consultation services.

Under no circumstances shall anyone not so authorized, attempt to repair any College-owned equipment or install or remove software.

Software Evaluation

Faculty will be held responsible for complete evaluation of software for their particular curriculum. All software should be approved by the Director of Technology to ensure compatibility with McDowell Technical Community College's computer systems. All software must be evaluated and approved two (2) months prior to the end of each semester. This will allow sufficient time for installation and seamless integration to MTCC's computer systems and allow the faculty members ample time to familiarize themselves with the new products.

Software Purchases & Licensing for Administrative, Faculty, and Staff Use

Microcomputer users must comply with laws governing the use and unauthorized duplication of copy-protected software. Employers must be able to demonstrate that any software they are using is by permission of the manufacturers; otherwise they are themselves at risk and are placing McDowell Technical Community College in a position to be heavily fined by the Software Publishers Association. McDowell Technical Community College disavows any authorized duplication or use of unauthorized copies of protected software.

To prevent unlicensed or unauthorized software on campus:

1. The Director of Technology / Information Systems must approve all purchase orders for software. Upon approval of the software purchase, the Director of Technology / Information Systems or his/her delegate will be responsible for ordering all software and maintaining a record of all software licensed for MTCC and to whom the copies are issued.
2. Each person or lab should have only one copy per computer of the licensed software available.
3. Software cannot be copied or loaned to students, staff, or faculty for their personal use.

Departmental Responsibilities for Use of College Computers

Any reports produced based on data that is maintained on any of the College computer systems will only be as valid as the data that is on file. All personnel must be aware that if invalid data is entered into the system, then reports based on this data will not be accurate. It is the personal responsibility of each employee to ensure that any data that he/she inputs is true and accurate to the best of their knowledge. Further, the validity of any report produced on the computer system assumes proper system interrogation on the part of the user.

Reporting requirements imposed on departments within the College by internal and external interests must remain the sole responsibility of the departments producing the report.

Data owners are as follows:

Human Resources (HR)	College President
Colleague Financials (CF)	Vice President of Finance and Administration
Student (ST)	Chief Academic Officer

The Director of Technology/Information Systems will assist users in producing reports and organizing data: however, the responsibility for correctness of the data and the final report, and the timeliness of the report, remains with the department from which the report was requested (data owner) and does not become the responsibility of the Technology Department.

Violations

Each individual is ultimately responsible for his/her own actions; failure to exercise responsible, ethical behavior will result in disciplinary action as appropriate. Disciplinary action may include reprimand or denial of access. In severe cases, employees may be subject to disciplinary action as determined by their immediate supervisor.

Certain activities violate federal and/or state laws governing use of computer systems, and may be classified as misdemeanors or felonies. Those convicted could face fines and/or imprisonment.

Agreement

All users of McDowell Technical Community College computer resources must read, understand, and comply with the policies outlined in this document. By using any of the College's computer resources, users agree to comply with these policies.

I have read, understand and agree to abide by the guidelines of the Acceptable Use of Computer Resources, Internet, and Network Policy.

Print Name:_____

Signature:_____Date:_____

McDowell Technical Community College

Colleague User Request Form

Employee Legal Name: _____

Title: _____

(Place an X next to the desired database)
Colleague Access: _____TEST _____PRODUCTION
Databases needed: _____ HR _____ST _____CF
Informer? (Y/N): _____
Communication Management? (Y/N)_____

PLEASE LIST MNEMONICS NEEDED

If there are special access needs that are not addressed above please specify below:

Supervisor Signature: _____ Date: _____

CF/HR Data Owner (VP of Finance) _____ Date: _____

ST-CU Data Owner (Vice President for Academics and Student Services) _____ Date: _____

ST-CE Data Owner (Vice President for Workforce Development) _____ Date: _____

****This form should be signed and returned to the Director of Technology****

Director IT Signature: _____ Date: _____

Setup by: _____ Date: _____

McDowell Technical Community College

IT SYSTEMS ACCESS REQUEST FORM

(Please print or type legal name of user as listed on his/her Social Security Card)

Name: _____
Last First Middle

Position Title: _____

Phone Extension: _____ Office (Building/Room): _____ Dept: _____

Job Status: _____Full-Time _____30-Hour w/Benefits _____Part-Time/Temporary

Please Check One: _____New Hire _____Existing Employee _____Position Change

PLEASE INDICATE THE SYSTEM ACCESS REQUESTED:

___Computer Requested ___ GroupWise Email ___ Faculty Access (Student Data Registration) ___Phone ___Voicemail

Datatel Access:
Collive:_____ Coltest:_____
Databases Needed:
Datatel ST:____ Datatel CF:_____ Datatel HR_____

Please complete Datatel User Request form also*

PLEASE INDICATE ANY NEEDS SPECIFIC TO THIS USER IN THE SPACE BELOW:

Employee:
I have read and accept the Use of Computer Resources, Internet, and Network Policy in the MTCC Policy & Procedure Manual. I will maintain the confidentiality of my password and ensure data integrity.

_____ _____
Employee Date

Access Approval:

_____ _____
Supervisor Date

For Information Services Use:

User ID :_____ Notes:
User ID (Unix):_____
GW ID_____
User Setup by:_____
Date Added:_____
Webmaster Notified (Date):_____
Domain Admin Notified (Date):_____

Director IT Signature: _____