Privacy, Safety & Security of Data: Acceptable Use Policy for Distance Learning

Table of Contents

Privacy, Safety & Security of Data

Introduction

The IT staff of the School District of Manatee County (SDMC) and Manatee Technical College (MTC) hold credentials in the following areas: server infrastructure, desktop infrastructure, private cloud, enterprise devised and apps, data platform, business intelligence, messaging and communication. This allows direct knowledge regarding best practices in technology infrastructure.

Data Storage & Network Access

The Administration of MTC manages all staff and student access to distance learning management systems. They work closely with SDMC IT staff to ensure that MTC is operating with a safe and adequate infrastructure.

MTC employees and students are provided with credentials to access the MTC and SDMC networks and are provided server space to store digital materials. When an employee is no longer a staff member or when a student is no longer enrolled, their access to the server and network is revoked.

Privacy, Safety, & Security Application and User Security

User Authentication: User data on our database is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on.

User Passwords: User application passwords have minimum complexity requirements.

Data Encryption: Certain sensitive user data, such as account passwords, are stored in encrypted format or masked to all but limited individuals with specific requirements for viewing.

Physical Security

Data Centers: MTC's information systems infrastructure (servers, networking equipment, etc.) for the distance learning management system is in a server facility off-site due to our managed hosting/SaaS system configuration. Some limited use servers are secured at the district level and are housed at the School District of Manatee County's secure datacenter, where they are monitored and maintained by district staff.

Data Center Security: The School District of Manatee County's data center is surveilled 24 hours a day, 7 days a week. Access is fully secured with district security entry requirements.

Environmental Controls: All district and MTC IT facilities are maintained at controlled temperatures and humidity ranges which are continuously monitored for variations. Smoke, fire detection and response systems are in place. Distance learning data is housed in a secure data facility.

Responsibilities of Institution

Introduction

The IT, instructional and administrative staff members of Manatee Technical College hold credentials in those areas of expertise that determine their responsibility to ensure the quality of distance education offered by the institution.

IT Staff Responsibility

The School District of Manatee County IT Department will maintain equipment designated for student use, will provide support to the network (local and district), and will work with MTC staff to ensure access to resources. They will communicate periods of down time, and will provide appropriate technical support at all levels, as requested through instructional faculty.

Instructional Faculty Responsibility

Manatee Technical College instructional faculty members will provide access to high-quality distance education curriculum that is aligned to state and industry standards. They will provide initial training on the use of the LMS, relevant to the specific course. The curriculum will be reviewed by an advisory panel of industry members and will use instructional materials that represent up-to-date and relevant theory within the discipline. The institution ensures timeliness of its responses (synchronously or asynchronously) to students' requests by placing a requirement on response times to no more than 24 hours during regular school hours. After school hours, holidays and weekend response will be outlined in course syllabi. Courses will be continually evaluated, both by the instructors and by administrators, to ensure that the elements of high-quality and standards-aligned online coursework are in place.

Responsibility of Administration

Manatee Technical College administration will review distance education courses for content and structure annually. They will communicate expectations for quality to instructors, participate in advisory meetings, and address student concerns as they related to distance education needs, in an impartial fashion.

Technology Requirements

When participating in distance education courses, it is vital to consider the technology needed in order to have a successful course. We recommend that you meet the technical requirements below when using any MTC learning management system (LMS).

Note: For additional required hardware or software requirements for your course(s), contact your instructor or refer to the course syllabus for additional information on their requirements.

Required Hardware

- A computer (desktop/laptop) or mobile device (smartphone/tablet) that is less than 5 years old will work.

NOTE: Chromebooks are not recommended and may not be compatible with all third-party tools used in course shells.

- Speakers/headphones/earbuds for listening to audio or videos presented in courses.
- Webcam for interacting in course activities that require video feedback from students (such as Studio), video test proctoring (such as Respondus), or other third-party tools.

Required Software and Connections

The following software is required:

- Google Chrome (latest version) - Download
- Adobe Acrobat Reader (latest version) - Download.
- Microsoft Office (includes Microsoft Word, Excel, and PowerPoint).
  Students have free access to install the suite on their computers. Find your Office 365 apps on your MTC Dashboard at https://www.MTCdashboard.net.
- Windows Media Player
- Internet Connection
  A stable Internet connection of 56K or greater is required. Please note that a 56K connection may degrade the quality of your experience.
- Internet Browser(s)

Various browsers may be able to access the learning management system. For more information, please visit specific requirements for the LMS used by your MTC program

Canvas requirements

Pearson requirements (NCCER and others)

Respondus LockDown Browser

Turnitin

Manatee Technical College has a license agreement with **Turnitin.com**, a service that helps detect plagiarism and the use of AI (i.e. ChatGPT, Bing AI, Chatsonic, Jasper Chat etc.) by comparing student papers with Turnitin's database and internet sources. Students who take this course agree that all required papers may be submitted to **Turnitin.com**. Papers submitted to Turnitin retain student copyright to the work they created. A copy of submitted papers is retained in a Turnitin database archive to be compared with future submissions—a practice that helps protect and strengthen copyright ownership. Use of the Turnitin service is subject to the Terms and Conditions of Use posted on Turnitin's website at **https://help.turnitin.com/Privacy_and_Security/Privacy_and_Security.htm**

Respondus

This course may require the use of Respondus LockDown Browser for online exams (remote and in-class). This is link unique for Manatee Technical College privately owned computers and laptops. For install on SDMC computers and laptops please contact your instructor who will contact IT support to use Installer for Managed Computers instead.

Acceptable Use Policy

Introduction

This document sets forth the policy of acceptable use by users of the learning management systems utilized by Manatee Technical College (MTC). Manatee Technical College currently uses Canvas and others as learning management systems (LMS), and this policy should be read in conjunction with the Terms of Use for your program's specific LMS. All users, including, but not limited to, students, teachers, school administrators, and educational organizations are subject to this policy and are expected to comply with its provisions.

User Responsibilities

It is the responsibility of any person using the LMS to read, understand, and comply with this policy. Any person with questions regarding the meaning of the policy, or application of this policy in a particular context, should seek clarification from the LMS administrator. For Canvas, questions may be directed to chamberlainl@manateeschools.net. Use of the LMS shall constitute acceptance of the terms of this policy.

Acceptable and Unacceptable Uses

The LMS is available only for educational purposes. Users may not use the LMS to store any files that are not educational.

It is unacceptable for users to use the LMS for:

- furthering any political or religious purpose.
- engaging in any commercial or fundraising purpose.
- sending or posting threatening, harassing, or disparaging messages or content to or regarding an individual or group of people.
- gaining unauthorized access to computer or telecommunications networks.
- interfering with the operations of technology resources, including placing a computer virus on any computer system, including an LMS;
- accessing or sharing sexually explicit, obscene, or otherwise inappropriate materials.
- intercepting communications intended for other persons.
- attempting to gain unauthorized access to any LMS;
- logging in through another person's account or attempting to access another user's password or files.
- sending defamatory or unfounded material concerning a person or group of people.
- furthering any criminal or illegal act, including downloading, uploading, or distributing any files, software, or other material in violation of federal copyright laws.

• infringing on any intellectual property rights; or

• downloading, uploading, or distributing any files, software, or other material that is not specifically related to an educational project.

The LMS may not be used to transmit or store messages or other data that are prohibited or inappropriate under this policy. Users may not create, send, or store messages or other data or content that are considered offensive, contain sexually explicit material, or otherwise offensively address the age, race, ethnicity, gender, gender identity, sexual orientation, religious or political beliefs, national origin, or disability of a person or a group of people. Users also may not create, send, or store messages pertaining to dangerous devices such as weaponry or explosive devices. Users should take all reasonable precautions against receiving or downloading messages, images, or other data of this sort.

Expectations Regarding Academic Integrity

Enrolled users will participate and submit required assignments as requested or required. The assignments submitted by users will represent their own work, or, where the work is not their own, the sources appropriately credited. Any user who is found to have submitted work that is not his or her own, either in whole or in part, and that has failed to credit the source, will be subject to one or more penalties. Penalties may range from loss of credit for the assignment to failure of the course, depending on the nature and severity of the act or omission. For further information, refer to MTC Student Handbook.

No Expectation of Privacy

Use of the LMS constitutes consent for administrators to monitor and/or inspect any files that users create, any messages they post or receive, and any web sites they access. MTC may inspect any user's account and the files it contains at any time. MTC also has the right to give permission to teachers, school administrators, law enforcement officials, and others, as appropriate, to review the LMS to determine the online activities of a user who MTC has reason to believe may be in violation of this policy. Users are advised that messages in discussion forums, including deleted messages, are regularly archived, and can be retrieved. In addition, an Internet firewall automatically checks all data moving between the local area network and the Internet and logs the sending and receiving destinations.

Passwords

Each user shall be required to either create or maintain the administrator-assigned password in a manner directed by the LMS vendor and shall use and maintain the password as directed by the same as set forth in this policy. This password is to be used to access the LMS computer network and any resources that reside within the network and require password access. LMS users are expected to keep their passwords confidential and are responsible for all activity under their accounts. If a user suspects their password has been compromised, they must notify their instructor, who will notify the LMS administrator.

Violations
Failure to comply with this policy may subject a user to termination of the user's LMS account. MTC will notify school or organization administrators of any inappropriate activities. It will also advise law enforcement agencies of activities conducted through the LMS which MTC believes may be illegal. MTC will cooperate fully with local, state, and/or federal officials in any investigation related to illegal activities conducted through the LMS.

Disclaimers
Manatee Technical College makes no warranties of any kind, either expressed or implied, for LMS services and resources. MTC is not responsible for any damages incurred, including, but not limited to: loss of data resulting from delays or interruption of service, loss of data stored on the LMS, or damage to personal property used to access LMS resources; the accuracy, nature, or quality of information stored on LMS resources or gathered through the LMS or the Internet; or unauthorized financial obligations incurred through LMS-provided access. Further, even though MTC may use technical or manual means to limit user access, these limits do not provide a guaranteed means for enforcing the provisions of this policy. All provisions of this agreement are subordinate to local, state, and federal laws.

Authentication of Academic Examinations

Introduction
MTC has several systems in place to ensure that examinations administered to students are completed by the same student who has registered for that course or program of study. Students are required to agree, in writing, to standards of academic integrity and to adhere to specific codes of student conduct; in addition, all students of Manatee Technical College are required to sign an agreement for Network/Internet Acceptable Use, prior to being permitted access to any electronic resources. Any additional fees charged to students to verify student identity shall be disclosed prior to the student's enrollment in the program.

Off-Site Exam Administration
When online students are required to take tests at a location other than at an MTC campus location, distance learning instructional personnel have several options for securing the test, including:

• Requiring the use of a separate password to access the examination

• Timing the exam

• Setting the exam to "turn on" and "turn off" within specific time frames

• Randomizing questions for each re-examination

• Limiting the location where the exam can be taken, based upon the IP address

• Employing remote proctoring technologies and software.

• Requiring the addition of a browser extension to a personal computer.

On-Site Exam Proctoring

For added security, distance learning instructional personnel also schedule on-site exams for students, and secure testing locations for those students to test when they arrive on-campus. In addition, there are testing centers on campus that have been established for specific industry certification testing purposes with certified proctors, to ensure the validity and authentication of such examinations, as required by the testing bodies.

APPENDIX A Academic Integrity Statement Form

Academic Integrity Statement

Each student enrolled in an online course will adhere to the academic integrity policy outlined below. Any violation of this policy will result in disciplinary action and may jeopardize the student's continuation in the course and any award of academic credit.

Each student will agree to abide by the following rules of academic integrity:

1. Your work on each assignment will be completely your own.

2. Your instructor must approve or assign any collaboration with another classmate on assignments and/or projects.

3. You will not practice plagiarism in any form.

4. You will not allow others to copy your work.

5. You will not misuse content from the Internet.

6. You will not represent work generated by artificial intelligence (AI) as my own or submit such work in a way that is inconsistent with the expectations of my teachers.

7. Each LMS account is for the use of the student to which it has been assigned and only for the use of that student.

Plagiarism is copying or using ideas or words (from another online classmate, or an Internet or print source) and presenting them as your own.

Remember that all instructors use many ways to check for authenticity. If an instructor confirms that a student has violated academic integrity, the student will be subject to consequences determined by the Code of Student Conduct policy of the school district where the student has enrolled.

I hereby agree to abide by the rules of academic integrity as stated above.

_____

Print Your Full Name Above

_____

Sign Your Full Name Above _____ Date

APPENDIX B:
PCS Network/Internet Acceptable Use Agreement Form

Technology and Internet Safety Policy

Technology is an integral part of your educational experience and must be used in a way that is consistent with the goals of the School District of Manatee County (SDMC). Technology includes, but is not limited to, computers, tablets, other electronic devices, software, email, the Internet, and other network resources. Your use of technology is a privilege and you are

responsible for using it appropriately. This includes use of district technology while off school property. The following are improper uses of technology:

a. Photographing, recording, or using images of any person without their knowledge or consent.

b. Accessing pornographic or obscene images, language, or materials, including screen savers.

c. Transmitting any material in violation of federal, state, local law, School Board policy, regulation, or the District Code of Student Conduct. This includes but is not limited to copyrighted material; threatening, obscene or pornographic material; test questions or answers; student work products; trade secrets; and computer viruses or malware.

d. Using technology for commercial activities unless explicitly permitted by the School Board.

e. Modifying the original SDMC pre-set software image including, but not limited to: loading software applications not authorized by SDMC; changing the computer name; changing or removing operating system extensions; altering security/filtering software; altering the preloaded operating system or application; or taking apart the computer for access to internal parts.

f. Downloading music, games, or videos at any time on a district computer.

g. Using cellular phones or other wireless communication devices during unauthorized times of the school day. Cellular phones, tablets, and other electronic devices may only be used on campus before or after school, unless your school has different policy on restrictions, or you have permission from an administrator or designee.

h. Using email, instant messaging, texting, web pages or other technology operations to threaten, disrupt, or interfere with the safety and welfare of the school community, including engaging in cyber-bullying, harassment, or "sexting."

i. Gaining or attempting to gain unauthorized access to SDMC networks, computer servers, or data files.

j. Gaining or attempting to gain unauthorized access to non-SDMC networks, computer servers, or data files utilizing SDMC equipment.

k. Using profanity, obscenity, or other language which may be offensive to another person, or reposting personal communications without the author's prior consent, when using computer network access.

l. Downloading or printing any material that is considered inappropriate by the School District.

m. Attempting to log on to the SDMC network or other district-affiliated systems using another's identity or password.

n. Sharing of logins and passwords to the SDMC network.

o. Bypassing or attempting to bypass SDMC filtering software.

p. Unauthorized disclosure use and dissemination of personal information regarding students, unauthorized online access by students, including hacking and other unlawful activities and access by students to inappropriate matter on the Internet is prohibited.

q. Follow this link for details regarding the use of social medial for School District of Manatee County students. Student Social Media Guidelines

NOTE: There is no right or expectancy of privacy on District provided or owned technology. School officials may review any information or files on such technology at any time.

I have read and understand the Technology and Internet Safety Policy as stated above.

_____

Print Your Full Name Above

_____

Sign Your Full Name Above

_____

Date

APPENDIX C:

Student Orientation to LMS

Getting Started with Canvas as a Student – watch this video to get started in Canvas

Canvas Student Guide

Canvas Login: Manateetech.instructure.com

NCCER Student Guide

APPENDIX D:

Instructure (Canvas) Privacy Statement https://www.instructure.com/policies/privacy

After you login to Canvas, on the very bottom of your Dashboard screen, there are a few links such as "User Research", "Privacy Policy", and "Terms of Service."

Pearson (NCCER and others) Privacy Statement https://www.pearson.com/en-us/legal-information/privacy-policy.html

Respondus Privacy Statement

https://web.respondus.com/privacy/privacy-additional-website/

Turnitin Privacy Statement

https://www.turnitin.com/privacy

ManateeTech.edu