Morgan County Board of Education

Monitoring:	Descriptor Term:	Descriptor Code:	Issued Date:
Review: Annually, in November	**Technology Acceptable Use and Internet Safety Guidelines**	**5.613**	**02/05/13**
		Rescinds:	Issued:

PURPOSE

Morgan County Schools provides employees access to electronic resources that promote educational excellence, sharing of information, innovative instruction, and online communication to enhance learners' ability to live and work in the 21st century.

- The purpose of these guidelines is to ensure that users recognize the procedures which the school imposes on their use of the MCS network (wired and wireless), MCS PODNet, the Internet, e-mail, and release of student information.
- They are provided to help understand what constitutes acceptable behavior with the use of technology.
- These rules and guidelines detail acceptable use of the networks, the Internet, and electronic information resources anywhere. All members of the MCS community (students and staff) are expected to comply with these standards.
- Due to the dynamic nature of technology, it is recommended that these guidelines be reviewed annually.

ELECTRONIC RESOURCES

These procedures are written to promote positive and effective digital citizenship among staff and are based on recognized Netiquette practices of respect, privacy, sharing, and safety.[1]

Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career.

They also recognize that expectations for staff behavior online is no different than face-to-face interactions.

EMPLOYEE COMPLIANCE

All employees must comply with all MCS Board of Education policies—including the Access to Electronic Resources and this Technology Acceptable Use & Internet Safety Guidelines policy.

ACCESSING THE MCS NETWORK

- Before any employee is allowed use of the MCS Network, that person shall sign a form that indicates his/her agreement to comply with the MCS Board policies Access to Electronic Resources and this Technology Acceptable Use & Internet Safety Guidelines policy. All employees agree to be bound by these policies even if no signed written form is on file.

- The required consent/agreement form indicates knowledge of and agreement to comply with the policies and procedures covered in the MCS Technology Acceptable Use & Internet Safety Guidelines and the MCS

Access to Electronic Resources.

MCS NETWORK ACCEPTABLE USE

Acceptable network use by district staff members includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Staff participation in blogs, wikis, collaboration groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;

Unacceptable network use by district students and staff includes but is not limited to:

- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material;
- Attaching unauthorized equipment to the district network.
- Cyber bullying, insulting, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Damaging computers, computer systems, computer networks or any device on the network
- Downloading, installation and use of games, audio files video files or other applications (including share ware or freeware) without permission or approval from the Morgan County Schools Technology Coordinator;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manu facture);
- Intentional misuse of resources;
- Liability or cost incurred by the district;
- Personal gain, commercial solicitation and compensation of any kind;
- Trespassing in another's folders, work, or files;
- Unauthorized access to other district computers, networks and information systems;
- Use of the network for commercial purposes;
- Using another's password or other identifier (impersonation);
- Using obscene or abusive language;
- Violation of copyright laws

USE OF PERSONALLY-OWNED DEVICES (PODS) IN SCHOOL

A personally owned device (POD) is a device that has the capability of connecting to a computer network (wired or wireless). A POD can be (but is not limited to) a camera, recorder, phone, player, game console, or computer with or without Internet capabilities. Such PODs may include (but are not limited to): CD/DVD players, iPads, iP0ds, MP3 players, tablets, game consoles, netbooks, laptop/notebook computers. PODS may be stored in backpacks, purses or personal carry-alls.

MCS WIRELESS NETWORK

Morgan County Schools offers wireless Internet access for personally owned devices (PODs) on all campuses within the district. This MCS PODNet Wireless Network operates alongside the MCS Wireless School Network and allows anyone with a wireless device to access the Internet on school grounds. The only difference between the two networks is that the MCS Wireless School Network allows access to all peripherals (including printers) and to files stored on network drives; MCS PODNet Wireless Network does not.

Each time a user accesses the MCS PODNet Wireless Network, that user agrees to the terms listed below:

1. Staff are expected to connect their PODs to the Internet via the MCS PODNet Wireless Network.
2. MCS will not be held liable for any damage that may occur as a result of connecting to the MCSPODNet Wireless Network or any electrical power source.
3. MCS will not be held responsible for any physical damage, loss or theft of the POD.
4. PODs brought on school property may be subject to search.
5. PODs will only be allowed at designated locations and/or times.
6. MCS will not be obligated to provide support, maintenance, or repair of any POD.
7. Student use of PODs in the classroom setting will be at the discretion of the principal or teacher.
8. Persons connecting PODs to the MCS PODNet Wireless Network must have a compatible network card con figured properly, and agree to maintain current anti-virus software enabled on their devices.
9. All activities while accessing the MCS Wireless School Network and the MCS PODNet Wireless Network are governed by the guidelines set forth in this policy and the Access to Electronic Resources policy.
10. MCS will not be obligated to supply electrical power access to power PODs where such access does not already exist.
11. Anyone bringing personal technology to school agrees to be responsible for and to reimburse MCS for any damage that they may cause arising out of and relating to the use of the MCS PODNet Wireless Network and his/her POD.

INTERNET SAFETY: STUDENT INSTRUCTION, STAFF PROFESSIONAL DEVELOPMENT, PARENTAL INVOLVEMENT

- Schools are to provide in Internet safety instruction to students in grades K thru 12.
- Internet safety professional development will be available to all teachers and administrators throughout the district.
- Outreach programs to families and community will be offered annually. Schools will use existing avenues of communication to inform parents about Internet safety.

INTERNET SAFETY: STUDENT SUPERVISION

- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.
- Although teachers will monitor student activity online and filtering software is in place in accordance with Children's Internet Protection Act (CIPA) regulations, it is the direct responsibility of students to comply with this acceptable use policy.

INTERNET SAFETY: DISPLAYING MEDIA CONTENT

- MCS allows media-type websites to display content to students through teacher access for educational use in the classroom using technology devices.
- Deliberate & consistent monitoring of this displayed content should include these guidelines:
    - Do not allow students to use a teacher login to the MCS network (for ANY reason).
    - Prescreen any video in its entirety BEFORE showing it to students.
    - When showing videos, make sure the display is in Full-Screen mode to avoid showing the comment section below the video, which sometimes has inappropriate language/remarks, and to avoid showing the peripheral ads, which may also be inappropriate.
    - Any online/downloaded videos should be viewed ONLY for educational resources. Specific state

standards (including Common Core) should be accomplished with the viewing of such videos. Teachers are expected to use their professional judgment when selecting media to use with students.
- Do not leave the room (even for a short time) while playing an online/downloaded video.
- Staff should not remain logged in to unattended workstations without locking them (Control L).
- MCS reserves the right to block any media website which is being misused.

INTERNET SAFETY: PERSONAL INFORMATION AND INAPPROPRIATE CONTENT

- Staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school or district web site unless the appropriate permission has been verified according to district policy.
- If users encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority or IT staff member immediately.

NETWORK SECURITY

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- All staff passwords will be changed at the beginning of each school semester.
- Do not use another user's account;
- Do not allow other user's access to your account;
- Keep your network password and other network account information confidential;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- The "remember password" feature of Internet browsers and other password-protected websites is a dangerous feature to use and should be avoided; and
- Lock the screen ("control, alt, delete" then "Enter"), or log off, if leaving the computer.

Any staff who suspects that someone has discovered his/her password should notify a network administrator to change it. Staff may change their network password at any time.

All network users may be monitored at any time by authorized personnel to assure compliance with these guidelines.

SAVING DOCUMENTS

Employees should save all documents to the network drive in their individual user's folder or cloud media Do not save any applications to the network: only documents and data. Due to server storage limitations, any applications or executable files residing in your user directory will be deleted. Any documents residing solely on your local computer are at risk. It is your responsibility to make sure important documents and data are saved to the network. All personal files on your computer(s) are solely your responsibility. This includes, but is not limited to: stored passwords, pictures, documents, or applications. In the event of a reload of the machine, either intentional or inadvertent, any locally stored data may be irretrievably lost. You are strongly encouraged to make and maintain regular backups of any data you choose not to store on your network drive.

Use of portable media devices (including mass storage devices) may be used to save files. Execution of programs from the portable media device is prohibited. In addition, portable media devices may not be used as

bootable media. Portable media devices brought on school grounds may be subject to search. Use of cloud storage sites approved by the technology department to save files is allowed.

E-MAIL

For Staff

MCS has provided an e-mail system for the internal and external communication of employees and board members. Responsible and ethical use of the e-mail system is required. The e-mail system may not be used for personal gain, or political or religious views or in any illegal, offensive or unethical manner. The e-mail system is intended only for valid and legitimate MCS-related communication.

MCS does reserve the right to access any e-mail for any business purpose, and also for inspection for disciplinary or legal actions. Your e-mail may be accessed with or without your knowledge. Deleting messages from your e-mail account folders will not prevent the IT department staff from viewing all mail sent to or from your account.

All e-mail is filtered for content. Email containing offensive words or themes will not be delivered. The IT staff may contact the sender, the recipient, or both; in addition to any other relevant authorities.

SOCIAL NETWORKING

1. District staff who have a presence on personal social networking websites are prohibited from posting data, documents, photographs or inappropriate information that is likely to create a material and substantial disruption of classroom activity.
2. District staff are prohibited from accessing personal social networking sites on school computers or during school hours except for legitimate instructional purposes.
3. The Board discourages district staff from socializing with students on social networking websites. The same relationship, exchange, interaction, information, or behavior that would be unacceptable in a non-technological medium is unacceptable when done through the use of technology.
4. Staff are allowed to use District approved social media for sites for school use only.

VIRUSES AND VIRUS PROTECTION

MCS IT Department will provide virus protection and related software for all workstations and servers. Virus protection and related software will be installed by authorized IT personnel unless otherwise approved by the IT Department.

These procedures are designed to safeguard staff e-mail accounts:

- Open e-mail attachments ONLY from individuals you know.
- If you suspect an e-mail message may contain a virus, do not send that message to anyone.
- The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted.
- If you feel your computer may contain a virus, contact the IT Department immediately.
- There are many virus hoaxes. Never delete system files from a computer in order to remove a potential virus without first checking with the IT Department to make sure the virus is valid and not a hoax.
- Before forwarding reported virus "warnings," first check with the IT Department to make sure the virus is valid and not a hoax itself.
- Do not open any e-mail attachments from anyone you do not know.

COPYRIGHT

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

VIOLATIONS

Violations of this policy or a procedure promulgated under its authority shall be handled in accordance with the existing disciplinary procedures of this District.

Legal Reference:

1. Internet Connectivity and Technology Tools Duxbury Public Schools Acceptable Use Guidelines," Duxbury Public Schools, Massachusetts, http://www.duxbury.k12ma.us/documents/AUG9-8-10.pdf, downloaded March 29, 2011, (Used with permission).