Technology

Acceptable Use Policy

The School is pleased to offer to its students, faculty, and staff access to the Internet in accordance with the terms and conditions of this policy. All users of the internet access must comply with the school's Acceptable Use Policy. It is important that all users understand the terms, conditions, and responsibilities associated with the use of the internet access. All users and parents of all users under the age of 18 are required to sign the Handbook Contract stating they carefully read and understand the terms and conditions of the Acceptable Use Policy and will comply with the policy while using the school's computer network resources. The Handbook Contract is a legally binding document and must be signed prior to the User accessing the Internet.

This policy governs the use of all computers, computer-based communication networks and all related information technology equipment administered by MSA. A user is defined as any person employed by MSA, which includes full-time, part-time, temporary, or contract employees, persons who are employed by contractors or subcontractors of MSA, and any other individuals who are authorized to access or use agency information systems including students, parents, prospective students, and project volunteers. The electronic communications and facilities of MSA are the property of the State and by using these facilities the user acknowledges consent to abide by this policy. These facilities and resources are to be used for School business purposes.

MSA has taken available precautions to eliminate controversial material. However, it is impossible for MSA to restrict access to all controversial materials. Parents/Guardians agree not to hold MSA responsible for materials acquired by students on the network. Parents/Guardians accept full responsibility for supervision of each child's Internet access if and when their use is not in a school setting. Further, Parents/Guardians full responsibility for their child's use of property of MSA. Parents give their permission for MSA to provide computer network and Internet access to each child and consent to the monitoring of each child's computer and Internet activities by MSA. All conditions of the Acceptable Use Policy also apply to the use of the dormitory network, DormNet.

CIPA

In December 2000, Congress enacted the Children's Internet Protection Act (CIPA). For any school or library that receives discounts for Internet access or for internal connections, CIPA imposes certain requirements. The CIPA requires that schools restrict employee and student access to the Internet. Under the CIPA, covered schools must have an Internet safety program which filters both adult and student access to visual depictions that are obscene or constitute child pornography. The program must also prevent students from accessing materials that are harmful to minors.

The school receives these discounts for Internet Access through the E-Rate program and is therefore in compliance with the CIPA. Key terms for this policy are defined by the Children's Internet Protection Act.

In compliance with CIPA 2008 updates, all students at the Mississippi School of the Arts are educated about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms and in cyberbullying awareness and response.

COPPA

The Children's Online Privacy Protection Act (COPPA), effective April 21, 2000, applies to online collection of personal information from children under the age of 13, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Final Rule issued by the Federal Trade Commission spells out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children privacy and safety online.

Education, Supervision and Monitoring

Technology is utilized extensively at MSA. Formal communication to students will be done via e-mail to student MSA e-mail accounts, assigned to each student upon entrance to MSA. Visits from college admissions representatives, scholarship and summer program opportunities, and college entrance test deadlines are announced electronically. Students who do not check their e-mail daily may miss important opportunities. Student and parent resources can be found on the MSA counseling website.

It shall be the responsibility of all members of the **Mississippi School of the Arts**' staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of The Technology Coordinator or designated representatives. The **Mississippi School of the Arts** or designated representatives will provide age-appropriate training for students who use the **Mississippi School of the Arts** Internet facilities. The training provided will be designed to promote the **Mississippi School of the Arts**' commitment to:

I. The standards and acceptable use of Internet services as set forth in **Mississippi School of the Arts**' Acceptable Use Policy;
II. Student safety regarding:
    a. the Internet;
    b. appropriate behavior while on online, on social networking web sites, and in chat rooms; and,
    c. cyber bullying awareness and response (see also the Anti-Bullying policy regarding expectations of electronic usage).
III. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Network and Computer Usage on Campus

The Mississippi School of the Arts campus computer network is referred to as MSANet. The optional network service in dorm rooms is referred to as DormNet.

The MSANet usage policies are designed to provide an environment that is consistent with the MSA mission and vision, Mississippi Department of Education (MDE) requirements, and federal/state laws. MSANet refers to devices attached to the entire computer network system at the Mississippi School of the Arts. MSANet includes but is not limited to the Local Area Network (LAN on campus), all MSA file servers, and access to the Internet.

MSANet facilities and network connections are for providing educational computing support to students, faculty, and staff. Under federal statutes and the sections of the Mississippi Code, which govern the use of these resources, all users must use the MSANet resources properly and for the purpose designated by the legislature. Students, faculty, and staff must follow all existing federal and state laws and MSA regulations and policies that apply, including those specific to computers, networks, and websites, and those that may apply generally to personal conduct.

MSA reserves the right to monitor the system for signs of illegal or unauthorized activity. Even though the MSA **Acceptable Use** Policy may not expressly prohibit an activity, such behavior may not be permissible. The Technology Coordinator may delete files deemed necessary. For questions related to appropriate use, contact the Technology Coordinator.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the **Mississippi**

School of the Arts online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Student Responsibilities

As MSANet account holders, students should:

1. Be owners of their data and keep account information confidential;
2. Provide a personal USB flash memory device for school use in storing personal files and moving them from one computer to another. Other marketing terms used for these devices are "thumb drive" or "jump drive;"
3. Be responsible for ensuring that their data is adequately backed up and protected against unauthorized access;
4. Notify the Office of Technology to change their personal password when they suspect it has been compromised:
5. Report suspected violations of technology guidelines to the Technology Coordinator.
6. **Remember**, no information stored, produced, or transmitted in any way on devices that contact the MSANet or DormNet networks is to be considered confidential or private in any way. **ALL** information is subject to monitoring and examination for appropriate content at any time. This **INCLUDES** personally owned disks or devices used in conjunction with the MSANet or DormNet networks. Any such item must be surrendered on demand to any school official that requests it for examination. This specifically includes the personal flash drives required by each student.
7. Remain in good standing as a student at the Mississippi School of the Arts. When students are suspended, or otherwise no longer in regular routine attendance, permission to use school resources may be removed, and access to the school and its systems may be denied until the student returns to school in good standing. Students who are dismissed or expelled automatically forfeit all access to school technological resources.

Personal Computers and Peripheral Devices

In general, students may not connect their own computers, peripherals, or technological devices to the MSA network. This includes such devices as external drives, iPods, cell phones, smart phones, digitizing tablets, etc. However, students may connect thumb drives to the system for purposes of storing and retrieving their own personal data.

If a student has a special school project that requires connection of non-MSA equipment or devices to the school network, the **Technology Coordinator** will aid on an individual basis. A student who needs such accommodations should meet with the technology coordinator well in advance of deadlines to seek permission and make arrangements for connection. The **Technology Coordinator** has the final authority to decide permissions on a case-by-case basis and set specifications and timelines for network access.

Students who choose to have their own computers in a dorm room must:

1. Provide the computer and all necessary accessories to allow it to function that is configured by the student and/or parent in compliance with safety protocols;
2. Understand that that the resources of the MSA technology staff are for official school purposes only and cannot install or repair equipment, hardware, or software on student computers;
3. Understand that it is <u>a privilege NOT a right</u> for a student to have a personal computer on the MSA campus;
4. Recognize that violations of MSANet policy may result in personal computers being sent home, loss of some or all computer privileges, and/or other disciplinary actions;
5. Ensure that real time antivirus software is installed, active, and kept up to date on all machines (Level III Violation);
6. Agree that MSA reserves the right to modify the system configuration to insure compatibility with network systems;

7. Agree to keep the operating system of the computer up to date by automatically applying all manufacturer's security updates as they are released (Level II Violation);
8. Seek permission from the Technology Coordinator before connecting any computer equipment to any location on either DormNet or MSANet, or before moving anything to a different location (Level I Violation).

DormNet—Dorm Room Internet Access

MSA provides free Internet access for educational purposes in academic areas throughout the campus, including the library that is located in Student Life Center. The same rules for student usage and conduct apply to this service as do the MSANet network.

Parents and students must agree to the following stipulations:

1. **MSA strongly advises that parents purchase and install a content filter similar to NetNanny or CiberSitter to help prevent access to inappropriate content. It is the sole responsibility of parents to ensure that their child does not use a personal computer to access inappropriate content.** Parents and students must comply with school policy, local, state, and federal laws.
2. The owner of the computer will be held liable for all activity that occurs on their device, even if it is by another person.

MSANet Policy Enforcement

To protect the MSANet resources and monitor proper usage of computer resources for educational purposes, the Technology Coordinator shall:

1. Investigate alleged abuses of computer resources;
2. Access the electronic files of its users as part of that investigation if there are indications that computer privileges have been violated;
3. Limit the access of users found to be using any computer systems improperly;
4. Administer disciplinary actions as directed by school administration for violations of MSA policies that may include the loss of some or all computer privileges and/or other disciplinary actions;
5. Act as a technical advisor to school administrators when they hear all cases involving student misuse of computer privileges;
6. Deny student access temporarily pending review when there is reasonable suspicion that student use may harm or do damage in the interim; and
7. Administer the technical aspects of all penalties for computer violations assigned by school administration.

Hardware

1. All personal computers (PCs), servers, workstations, printers, network switches, and other associated equipment are the property of the State of Mississippi and should not be used for purposes other than school business. All such equipment is by default considered to be under the authority and supervision of the MSA Office of Technology unless it is specifically excluded in a written agreement between the MSA Office of Technology (MSAOT) and the appropriate substitute designee. No hardware changes, modifications, additions to, deletions from, or removal of any equipment may be done to any such style equipment without notification to the MSAOT in writing, including all units as described above. Additionally, any person other than Office of Technology personnel may make no such hardware changes to any unit under its supervision unless an MSAOT representative authorizes such action in writing in advance.
2. No personal devices are to be connected to the MSANet network without special permission for the MSAOT. The only routine exception to this rule is that personal USB Flash Memory devices (jump drives or thumb drives) may be used for storing or moving user data files.
3. The transfer of any information system equipment from one user to another, or to vendor for repair, must be recorded using appropriate MDE Property Office procedures.
4. Except for notebook PCs used daily in offsite work, no information systems equipment should be removed from the MSA premises without the prior permission of both the individuals' immediate

supervisor and the MSAOT. In the event equipment is to be off-premises for some time, the user responsible for the equipment must file a written notification with the Office of Technology.

Software

1. Software owned or licensed by MSA may not be copied to alternate media, distributed by e-mail, transmitted electronically, or used in its original form on other than MSA computers without express prior written permission from the MSAOT. Users will adhere to all applicable licensing agreements and copyright provisions.
2. Software licensed to MSA is to be used for its intended purpose according to the license agreement. Users are responsible for using software in a manner consistent with the licensing agreements of the manufacturer. License agreements are to be maintained by the MSAOT staff, or the machine's official substitute designee. Copies of all license agreements are to be kept on file in the MSA Technology office regardless of official supervisory authority.
3. Without prior written approval, software, including but not limited to Internet downloads, utilities, add-ons, programs (including shareware, freeware and Internet access software), patches, or upgrades, shall not be installed on any school owned equipment by anyone other than a representative of the MSAOT.
4. All software obtained for use on MSA equipment must be approved in writing by the MSAOT staff prior to acquisition. Any software obtained for systems that have a substitute supervisory designee must have a copy kept on file in the MSAOT Department along with the proof of the licensing certification.
5. Standard software is to be used for all internal functions. When required, approved non-standard software is to be used only to interface with customer/vendor organizations and other governmental agencies. Any non-standard software needed to perform a specific job function should be approved by the MSAOT.

Practices

1. System identification codes and passwords are for the use of the specifically assigned user and are to be protected from abuse and/or use by unauthorized individuals. Users are to use their individually assigned system access codes at all times, and are not to share codes. Any use of another user's code must be reported immediately to the MSAOT staff.
2. All e-mail attachments and executable e-mail messages are automatically scanned for viruses using the virus detection software installed on all MSA computer workstations. In the event of any configuration changes to the workstation, even with the approval of the MSAOT Staff, it is the responsibility of the user to ensure virus protection is active prior to opening/executing any file, regardless of the method by which it was obtained. In addition, users are expected to exercise good judgment and safe computing practices to protect agency systems against the threat of potential virus exposure.
3. Like all MSA information systems resources, Internet access and e-mail are for work-related use. Access to e-mail and Internet sites visited can be monitored at the specific individual level.
4. All Internet use facilitated by the MSANet system must conform to all regulatory statutes as governed by the Child Internet Protection Act (CIPA) and the Children's Online Privacy Protection Act (COPPA).
5. Users may not use MSA information systems resources for soliciting, personal financial gain, partisan political activities or further disseminating "junk" e-mail such as chain letters, spam, etc.
6. Information contained on any school system is strictly proprietary to the State of Mississippi and MSA. Copying or disseminating any of this information for any purpose other than state business is strictly prohibited.
7. It is highly recommended that all faculty and staff users store data files (word documents, spreadsheets, databases, etc.) in their various directories on the network fileservers. The MSAOT Department is responsible for backing up data on the network servers. The individual users are responsible for backing up any files not stored in the appropriate areas of the network servers.

Prohibited Communications

Electronic media cannot at any time be used for transmitting, retrieving, storing or disseminating any communication that is:

1. Discriminatory or harassing;
2. Derogatory to any individual or group;
3. Obscene or sexually explicit;
4. Defamatory or threatening; or
5. Engaged in for any purpose that is illegal, (including but not limited to file sharing of copyrighted materials with unauthorized users)
6. Engaged in for any purpose that is contrary to MSA's policies or interests.

Furthermore, users are prohibited from:

1. Visiting obscene web sites;
2. Participating in any obscene "chat room" communications;
3. Unauthorized monitoring or intercepting the files or electronic communications of other users;
4. Attempting to bypass any Internet filtering, traffic regulating, or such automated systems designed to control the access level and functionality of the MSA network as required by CIPA (Child Internet Protection Act);
5. Hacking or obtaining access to systems or files they are not authorized to use;
6. Using someone else's login or password.