MILES AHEAD CHARTER SCHOOL

Acceptable Use of Technology Guidelines

These Acceptable Use Guidelines govern the use of computing systems, technology, and facilities located at or operated by Miles Ahead Charter School ("MACS").

The definition of MACS information and data resources includes any computer, server, network, portable, mobile, cloud resources, or other electronic device provided by MACS, or access provided or supported by MACS, including the Internet. Use of the computer facilities includes the use of data/programs stored on MACS computing systems, data/programs stored on magnetic tape, CD-ROMs, DVD-ROMs, computer peripherals, or other digital storage media, that is owned and maintained by MACS.

The "user" of the system is the person requesting an account (or accounts) in order to perform work in support of MACS programs or a project authorized for MACS. The purpose of these guidelines is to ensure that all MACS technology users share MACS' technology resources in an effective, efficient, ethical, and lawful manner. Users that do not adhere to MACS' Acceptable Use Guidelines will have access to MACS technology and enterprise systems terminated.

Employees who violate the Acceptable Use Guidelines will be subject to disciplinary action, up to and including termination. Students who violate the Acceptable Use Guidelines will be subject to appropriate disciplinary action.

Accessing the Enterprise Network and Instructional Resources

MACS' Enterprise Network (EN) provides access to a wide variety of instructional resources that enhance the educational opportunities of its students. Use of EN resources must be in support of, and consistent with the vision, mission, and goals established by MACS' Governing Board in furtherance of MACS' charter contract. All users of the EN must maintain strict compliance with all applicable ethical and legal rules and regulations regarding access and use.

MACS encourages the use of the Internet, hardware, and software tools to support teaching and learning. It is the responsibility of each teacher to verify that the resources he/she chooses are related to MACS' educational program and curriculum and aligned with the mission and vision of MACS.

Harmful and Offensive Material

Given the nature of world-wide access to the Internet, MACS is not able to control all information available to be accessed by users of MACS' EN and devices. Some of the information that can be accessed via the Internet may be inaccurate, defamatory, obscene, profane, sexually explicit, threatening, racially offensive, or otherwise objectionable. MACS strongly encourages parents to discuss the appropriate access of information and materials with their students.

Students who violate the Student Code of Conduct in relation to access and/or distribution of harmful or offensive materials may be subject to disciplinary action.

The Children's Internet Protection Act and Family Education Rights and Privacy Act & the Protecting Georgia's Children on Social Media Act of 2024

In compliance with the Children's Internet Protection Act (CIPA), and the Protecting Georgia's Children on Social Media Act of 2024, MACS adopted and implemented an internet safety policy addressing:

1. Access by minors to inappropriate matter on the Internet;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including "hacking," and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
5. Measures restricting minors' access to materials harmful to them.

These Acceptable Use Guidelines and other MACS policies, procedures, and operating guidelines, complies with CIPA and the Protecting Georgia's Children on Social Media Act of 2024 as follows:

1. MACS blocks or filters content over the Internet that MACS considers inappropriate for minors by utilizing "Technology Protection Measures," as that term is defined in Paragraph (a)(4) of U.S.C. § 54.520 and Paragraph (a)(9) of O.C.G.A. § 20-2-324. This means that MACS uses software programs and controls to block inappropriate content including, but not limited to, pornography, obscene material, and other material that may be harmful to minors. MACS may also block, or filter other content deemed to be inappropriate, lacking educational or work-related content or that poses a threat to the

network. MACS may, in its discretion, disable such filtering for certain adult users for bona-fide research or other lawful educational or business purposes.

2. MACS prohibits students from accessing social media platforms through the use of computer equipment, communications services, or internet access that is operated, owned, leased, and made available to students by MACS.
3. The Executive Director may, in his or her discretion, permit students to access social media platforms only:
   a) For the exclusive purpose of accessing and utilizing age-appropriate educational resources;
   b) Under the supervision of such MACS personnel; and
   c) During the course of a MACS related activity.
4. As part of its annual technology needs assessment, MACS regularly evaluates and updates the use of technology solutions to aid in the prevention of cyberbullying on MACS equipment, including, but not limited to, monitoring software intended to provide electronic notification when the occurrence of cyberbullying is detected on such equipment.
5. MACS educates students and minors about digital citizenship and safe and appropriate use of technology, including interacting with other individuals on social media websites and in chat rooms and cyberbullying awareness and response. MACS implements programs modeled on the Georgia Department of Education's program to educate students regarding online safety in accordance with O.C.G.A. § 20-2-149.
6. Users, including minors, may not access inappropriate material as doing so is in violation of MACS' policies, procedures, or guidelines.
7. MACS works to protect the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
8. MACS works to prevent the unauthorized access, including "hacking" and other unlawful activities by minors online.
9. MACS works to prevent the unauthorized disclosure, use, and dissemination of personally identifiable information regarding minors. The Family Educational Rights and Privacy Act ("FERPA") is a federal law that protects the privacy of education records. Under FERPA guidelines, parents or eligible employees have the right to inspect and review the students' education records maintained by MACS.

Content Filtering

MACS maintains an Internet filtering system that includes filtering categories. The Information Technology Department maintains a list of Internet filtering settings by category that have been deemed appropriate based on a review by MACS staff.

Teachers are expected to monitor usage of technology in the classroom. All Internet-based activities should be conducted using MACS' network to allow for filtered access that is appropriate for student use. MACS staff may request a site be unblocked if it has been determined to be free of visual depictions that are: (i) obscene, (ii) child pornography, or (iii) harmful to minors, and the site is to be used for instructional purposes.

Users shall not use any website, application, or methods to bypass filtering of the network or perform any other unlawful activities. Examples include unapproved third-party VPNs and Proxys, used to bypass content filters.

Enterprise Network Access

The existing Enterprise Network (EN) is exclusively intended for MACS employees, students, and guests using MACS-approved and/or issued devices, tools, and/or applications. It is acceptable to provide guests with temporary guest login accounts for personal computers, tablets, and mobile devices used onsite by MACS stakeholders such as visitors, vendors, parent liaisons, or volunteers.

Copyright Considerations

Many written materials, including those widely available on the Internet, are the personal property of the author or other persons. Copyright laws protect these ownership interests and encourage the creativity of others. It is not always possible, particularly in the midst of classroom activity, to know whether a particular material is protected by copyright laws and, if so, whether a particular use is permitted as "fair use." Therefore, students and employees should assume that any material accessed on MACS' EN is the property of another and that use of the material is restricted by copyright laws. Material downloaded from MACS EN should not be distributed to others unless such permission is obtained from the owner of the copyright or his/her authorized representative.

Users shall not upload computer programs or software of any kind onto the EN unless they obtain permission in advance from authorized MACS personnel. MACS does not accept responsibility for violation of copyright laws by employees, students, or other users.

Public Posting

Messages can be posted on the Internet from computer systems around the world. MACS does not have control over the content of messages posted from external systems. MACS staff will determine which discussion boards, blogs, wikis, and groups are most beneficial to the educational mission of MACS. Use of external content not approved by MACS staff is prohibited. Messages posted locally may be removed by MACS personnel if they are in violation of MACS policy, procedures, or MACS rules. Misuse of discussion boards or groups may result in termination of the user's access and/or other disciplinary measures.

Real-time Interactive Communications (Video Conferencing)

Students, employees, and other users are expected to use the real-time conference and communication features of MACS' EN for educational or work- related communications only. Users must abide by any restrictions posted on the EN regarding interactive communications.

Use of the Internet and Electronic Mail (E-Mail)

Users will comply with all Federal and State laws, and MACS policies when accessing their MACS accounts. This includes, but is not limited to, the following requirements:

1. User accounts may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, cyberbullying, forgery, impersonation, gambling, soliciting for illegal pyramid schemes, unauthorized access to the systems, data, or network of MACS or a third party (including "hacking"), and/or service disruptions (e.g. spreading computer viruses and/or denying services).
2. User accounts may not be used in any way that violates MACS policies, procedures, or operating guidelines. Users engaging in online behavior that is not consistent with the mission of MACS, that misrepresent MACS, or that violate any MACS policy is prohibited.
3. The Enterprise network may not be used for unsolicited mailings unrelated to MACS' educational programs, access for unapproved users to MACS resources or enterprise network facilities, or competitive commercial activity unless pre-approved by MACS Governing Board.
4. Users may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to MACS or another individual without authorized permission.
5. In the interest of maintaining network performance, users should refrain from sending unreasonably large e-mail attachments.

6. Accessing wireless “hotspots” with MACS technology at public and/or unsecure locations should be avoided to prevent the breach of confidential data and information.

Transmission and Storage of Confidential Information

It is the responsibility of all MACS’ employees and contractors to protect sensitive data, and personally identifiable information (PII) in a professional and legally compliant manner. MACS’ employees and contractors will not be granted access to sensitive information that is not authorized based upon a job-related need to know or for a job-related legitimate educational purpose. This includes accessing data on MACS’ devices as well as devices containing MACS’ data owned or rented by employees and contractors. Confidential information includes, but is not limited to:

1. Student or parents name, address, telephone number, and social security number;
2. Student ID, grade, attendance, medical, or transcript information;
3. Student or parent financial aid or similar financial information;
4. Race/Ethnicity, birth date, age;
5. Employee name, address, telephone number;
6. Employee payroll and benefits information; and
7. Any information which by itself or if combined with other information would allow a person to be able to identify an individual.

Monitoring the Enterprise Network, E-mail, and Internet Usage

Use of the Enterprise Network (EN) is limited to the support of MACS’ educational mission. As such, information transmitted or received over MACS’ EN (including e-mail) should not be considered "personal" or "private." No user shall have an expectation of privacy regarding his or her use of MACS’ EN. Messages may be monitored and reviewed by MACS administration under the authority of the Executive Director without the consent of the sender, recipient, or intendent recipient. MACS may facilitate the access of information or communications to appropriate local, state, or federal officials in connection with their authorized activities. Additionally, information accessed or shared over MACS’ EN may be subject to disclosure under the Georgia Open Records Act. As a result, utilizing the EN to exchange confidential information should be minimized and additional protective measures, such as encryption, should be utilized when confidential information must be exchanged through the EN.

Users that do not adhere to appropriate use of the EN may have privileges terminated and may be subject to disciplinary action.

Charges

Use of the Enterprise Network (EN) in the manner permitted by MACS should not generate any additional costs or charges for MACS. Therefore, users will not be charged for such use. However, if the EN is used in a manner that is not allowed by MACS, the users engaged in such disallowed uses will be required to pay all costs incurred. In addition, misuse of the EN in this manner may result in loss of access or other appropriate disciplinary action.

Devices

Portable, mobile, hand-held, or other electronic devices and/or associated accessories for these devices should be used solely to support the vision and mission of MACS. Usage of MACS-issued electronic devices will comply with all Federal and State laws, and all MACS policies, procedures, and operating guidelines, including, but not limited to, the following:

1. Devices may not be used for illegal or unlawful purposes, including, but not limited to, obscenity, libel, slander, fraud, defamation, harassment, intimidation, impersonation, gambling, or soliciting for illegal pyramid schemes.
2. Devices may not be used in any way that violates MACS policies, procedures, or operating guidelines. Use of a device in a manner that is not consistent with the mission of MACS or that misrepresents MACS is prohibited.
3. Information transmitted or received utilizing MACS devices may be monitored and reviewed by MACS administration under the authority of the Executive Director without the consent of the sender, recipient, or intendent recipient. MACS may facilitate the access of information or communications to appropriate local, state, or federal officials in connection with their authorized activities. Additionally, information accessed or shared utilizing a device may be subject to disclosure under the Georgia Open Records Act.

Use of MACS-issued devices in the manner permitted by MACS should not generate additional costs or charges to MACS. Therefore, users will not be charged for such use. However, if MACS-issued electronic devices are used in a manner that is not permitted, the users engaged in such disallowed uses will be required to pay all costs incurred. Misuse of MACS-issued electronic devices may result in a loss of access privileges and appropriate discipline action. Users who are issued a device are expected to exercise reasonable caution in conducting business related communications. Hands-free devices must be used when driving. Texting while driving is strictly prohibited.

Electronic devices that are issued to employees are the responsibility of that employee. Electronic devices that are damaged under normal wear and tear by employees will be replaced at no cost. Employee devices that are otherwise damaged will be replaced at the discretion of MACS and the employee responsible for that device may be required to reimburse MACS for some or all of the replacement cost at the discretion of the Executive Director. Users must surrender MACS issued equipment immediately upon request. If the user is unable to present the equipment in good working order, MACS shall require the user to reimburse MACS for the cost of a replacement device.

User Identification Information

MACS may occasionally require new or updated information from users. Users must provide all such information as requested. Users also must notify the administration of any changes in user identification information (address, phone, name, MACS enrollment, etc.).

Use of passwords to protect information: MACS Enterprise Network

Passwords are an important method of protecting EN access and preventing unauthorized access to data. Therefore, sharing your passwords, attempting to log on to the EN using another person's password, falsely posing as another MACS user, or engaging in other security violations will be grounds for termination of privileges and other disciplinary measures. Users must immediately notify an administrator if their password is lost or stolen or if they believe that someone has obtained unauthorized access to their account password. The following requirements will apply to all passwords used for computer logon, email access, employee portal, and all single sign-on applications that utilize the same password. MACS password guidelines apply to all staff, students, contracted employees, and anyone using a user account provided by MACS.

1. Passwords must be changed every 60 days. You will be prompted when you log on to make this change;
2. Passwords are a minimum of eight (8) characters long;
3. New passwords cannot match any of the previous twelve (12) passwords used;
4. Passwords cannot contain part of the user's name or login name;
5. Passwords must meet all the following complexity requirements:
    a. Contain at least one uppercase letter (A through Z);
    b. Contain at least one lowercase letter (a through z);
    c. Contain at least one number or one special character (for example:0 through 9 or $, #,%)

   d. Contain at least one special character (for example: $, #, %,)
6. A user account will lock after five (5) consecutive invalid login attempts and will remain locked for 15 minutes. The account will automatically unlock after 15 minutes and allow login attempts to the account again.

Vandalism

Computer vandalism is prohibited and will result in disciplinary actions. Prohibited conduct includes creating computer viruses, service disruptions, harming or attempting to harm or destroy MACS' hardware, software or data; harming or attempting to harm the data of another user, the EN or any of the agencies or other networks that are connected to MACS EN; and harming or attempting to harm the hardware, software, or data of a third party. Abuse of a computer system may be subject to criminal penalties under state and federal law.

Reporting Loss or Theft of Equipment or Data

Users who possess MACS owned computers, devices, and accessories are expected to secure them whenever they are left unattended and it is the user's responsibility to protect the device and data. In the event a MACS-owned computer, device, or their accessories are lost or stolen, the user must report the loss or theft to a MACS administrator immediately.

Public Access to Technology Policies

MACS shall publish on its website a copy of its social media policy.

Rights of Parents and Legal Guardians of MACS Students

In compliance with the Protecting Georgia's Children on Social Media Act of 2024, MACS provides certain rights to parents and guardians of current students regarding student technology use. These rights include, but are not limited to, the following:

1. Reasonable opportunities and procedures to collaborate with MACS administrators and teachers regarding appropriate internet access for such students;
2. The ability to request information from personnel about what social media platforms MACS has permitted or intends to permit students to access;
3. The ability to prohibit their child from accessing one or more social media platforms MACS has permitted or intends to permit students to access;
4. Upon written request of a parent or guardian, access to a paper copy of the acceptable-use policy and the social media policy adopted by MACS and information regarding the administrative procedures in effect to enforce such policies and to address complaints about such enforcement.

Termination of Privileges

An employee's access to, and use of, the EN will be discontinued when he or she separates from employment at MACS. A student's access to, and use of, the EN will be discontinued when the student is withdrawn from MACS. Any user's access to MACS may be suspended or terminated for any action that violates federal or state law or MACS' policies, procedures, and operating guidelines.

Violations of these Guidelines

Failure to follow these guidelines can violate O.C.G.A. §§ 16-9-90 through 19-9-93 as well as the Children's Internet Protection Act and the Protecting Georgia's Children on Social Media Act of 2024. As a result, failure to follow these guidelines can lead to disciplinary actions, up to and including termination of employment, expulsion, and criminal prosecution. Administrative procedures for violations of the Acceptable Use of Technology Policy by students will adhere to the procedures described in the Student Hearing Procedure/Disciplinary Tribunal Handbook Policy. Administrative procedures for violations of the Acceptable Use of Technology Policy by MACS employees will adhere to the procedures described in the Personnel Progressive Discipline Policy.

Adopted: April 23, 2026