# Madison County Schools
# Student Technology
# Handbook

## Contents

# Technology Plan Implementation

Schools of the information age must effectively employ technology to better meet the needs of students, parents, teachers, and administrators. Since the Madison County Schools (MCS) completed its first written technology plan in May 1996, it has had an outline of very specific technology goals, along with objectives and strategies to reach those goals.

## Technology Goals

Equip all stakeholders to use technology to positively impact and interact with the world around them.

- Teach digital citizenship.
- Integrate technology seamlessly in the teaching and learning process while ensuring that the use of technology adds value to learning.
- Develop a new set of knowledge and skills for the 21st-century learner.
- Provide greater access to educational opportunities and differentiated instruction by utilizing access to technology for anytime, anywhere learning.
- Improve communication and widen our sense of community by expanding the way teachers, students, and parents are able to interact with each other.
- Integrate digital tools for students to develop products demonstrating their understanding.
- Provide greater access to digital content in a variety of formats and modes.

## Acceptable Use Policy

Madison County Schools (MCS) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. The District is committed to helping students develop progressive technology and communication skills.

MCS is committed to providing educational opportunities for all students and maintaining compliance with the Individuals with Disabilities Education Act 2004 (20 U.S.C. 1400 et seq.).

To that end, the District provides the privilege of access to technologies for student and staff use.

This Acceptable Use Policy (AUP) outlines the guidelines and behaviors that all users are expected to follow when using school technologies or when using personally-owned devices on school property, including:

- The Madison County Schools network is intended for educational purposes.
- All activity over the network or use of District technologies may be monitored, documented and retained.
- Access to online content via the network may be restricted in accordance with District policies and procedures and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Using an Internet filter and other technologies. The District makes a reasonable effort to

ensure students' safety and security online, but it will not be held accountable for any harm or damages resulting or arising from use of MCS technologies.

- Users of the District network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.
- User have no expectation of privacy.

**Technologies Covered**

MCS may provide the privilege of Internet access, desktop computers, mobile computers or devices, video conferencing capabilities, online collaboration capabilities, message boards, email, and more.

This Acceptable Use Policy applies to both District-owned technology equipment utilizing the MCS network, the MCS Internet connection, and/or private networks/Internet connections accessed from District-owned devices at any time. This AUP also applies to privately-owned devices accessing the MCS network, the MCS Internet connection, and/or private networks/Internet connections while on school property or participating in school functions or events off campus. MCS policies outlined in this document cover all available technologies now and in the future, not just those specifically listed or currently available.

**Usage Policies**

All technologies provided by the District are intended for education purposes. All users are expected to use good judgment by following the MCS student code of conduct and social media policy. Users should be safe, appropriate, careful, and kind; should not try to disable or get around technological protection measures; use good common sense; and ask if they don't know.

**Internet Access**

MCS provides its users the privilege of access to the Internet, including web sites, resources, content, and online tools. Access to the Internet will be restricted as required to comply with CIPA regulations and school policies. Web browsing may be monitored, and web activity records may be retained indefinitely.

Users are expected to respect the web filter as a safety precaution, and shall not attempt to circumvent the web filter when browsing the Internet. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, the user should submit a request for website review through the MCS Technology Help Desk or restricted access screen.

**Email**

MCS provides faculty, staff and students in grades 3-12 with the privilege of email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

Users provided with email accounts should use these accounts with care. Users should not send personal information and should not attempt to open files or follow links from unknown or untrusted origins. Users should use appropriate language and should only communicate with other people as allowed by District policy or the teacher or administrator.

Users are expected to communicate with the same appropriate, safe, mindful, courteous manner online as offline. Email usage may be monitored and archived.

## Device Usage

MCS may provide users with laptops or other devices to promote learning outside of the classroom. Users should abide by the same Acceptable Use Policies when using school devices off the school network as on the school network.

Users are expected to treat the devices with extreme care and caution; these are expensive devices that the District is entrusting to users' care. Users should immediately report any loss, damage, or malfunction to IT staff. Users will be financially accountable for any damage resulting from negligence or misuse.

Use of District-issued devices off the District network can be monitored.

## Policy

In some cases, a separate network may be provided for personally-owned devices. Please remember, this Responsible Use Policy applies to privately owned devices accessing the MCS network, the MCS Internet connection, and private networks/Internet connections while on school property.

## Security

Users are expected to take reasonable safeguards against the transmission of security threats over the MCS network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. Users should never share personal information.

If users believe the device they are using might be infected with a virus, they should alert IT. Users should not attempt to remove the virus themselves or download any programs to help remove the virus.

## Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use known or trusted sources when conducting research via the Internet.

Users should remember not to post anything online that they would not want students, parents, teachers, or future colleges or employers to see. Once something is online, it cannot be completely retracted and can sometimes be shared and spread in ways the user never intended.

## Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online.

Information obtained via the Internet should be appropriately cited, giving credit to the original author.

## Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others. Users should never agree to meet in person someone they meet online without parental permission.

If users see a message, comment, image, or anything else online that makes them concerned for their personal safety or the safety of someone else, they should immediately bring it to the attention of an adult (teacher or administrator if at school, parent if using the device at home).

## Cyberbullying

Cyberbullying including, but not limited to, harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking will not be tolerated. Users should not be mean or send emails or post comments with the intent to harass, ridicule, humiliate, intimidate, or harm the targeted student and create for the targeted student a hostile school environment.

Engaging in these behaviors or in any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Users should remember that online activities may be monitored.

All students will be educated about appropriate online behavior, including interacting with other persons on social networking websites and in chat rooms, and cyberbullying awareness and response.

## Social Media Policy

The District has a separate Social Media Policy that applies to all employees and may have implications for students. By signing the Acceptable Use Policy, users are acknowledging they have read the Social Media Policy and agree to abide by its requirements. Violations of the Social Media Policy are violations of the Responsible Use Policy.

## Examples of Responsible Use

I will:

- Use school technologies for school-related activities.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher, administrator, or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use District technologies at appropriate times, in approved places, for educational pursuits.

This is not intended to be an exhaustive list. Users should use their own good judgment when using District technologies. You can also visit www.commonsensemedia.org for further information.

## Limitation of Liability

MCS will not be responsible for damage or harm to persons, files, data, or hardware.

While MCS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

MCS will not be responsible or liable for, financially or otherwise, for unauthorized transactions conducted over the MCS network.

Violations of this policy may have disciplinary consequences, including:

- Suspension of network, technology, or computer privileges;
- Notification of parents;
- Detention or suspension from school and school-related activities;
- Employment disciplinary action up to and including termination of employment;
- Legal action and/or prosecution.

Employees, students, and parents/guardians shall be required to sign the District's Acceptable Use Policy annually before Internet or network access shall be allowed.

# Device Policy

**Terms**
Parents of students who are assigned a take home device shall pay a non-refundable annual usage fee as listed under "Fee for Device Use" on page 7. Users will comply at all times with the MCS Student Technology Handbook policies. Any failure to comply may result in termination of user rights of possession effective immediately and the District may repossess the device. Any lost, stolen and damaged device must be reported to school authorities immediately.

**Title**
The District has legal title to the property at all times. The user's right of possession and use is limited to and conditioned upon full and complete compliance with this agreement, the MCS Student Technology Handbook policies, and all District policies and procedures.

**District Hotspot**

If you have been provided a district owned hotspot, you understand and agree to the following:

- Any device (both personal and district owned) may be allowed to connect to the device.
- For personal devices (those not provided by the District), hotspots will provide basic internet filtering only, in compliance with the Children's Internet Protection Act (CIPA). No other filtering will be provided and/or controlled by the District for personal devices connected to the hotspot.
- District-provided devices will have additional filtering using District-provided filtering systems.
- Use of the hotspot is permitted only by students for educational purposes.
- The District will monitor any and all usage of the hotspots, including but not limited to the types of data used. Any data usage through the hotspot (including by personal devices) may be monitored by the District, and no data that passes through the hotspot is private.
- The District may, at its discretion, limit the speed or amount of data available through the hotspot.
- The District may also turn off the hotspot, disconnect service to the hotspot, or require return of the hotspot, at its sole discretion.
- The District is providing the hotspot as-is as a courtesy, and makes no promises or guarantees as to the availability or quality of internet connection available through the hotspot.
- Students and parents may be held responsible for any damage (accidental or otherwise) to the hotspot.

**Loss, Theft or Full Damage**
If a device is damaged, lost, or stolen, the student or parent/guardian should immediately notify the police, school administration and complete the District "Lost or Stolen Report" located at www.madison-schools.com. At that time, the parent/ guardian must file a police report. If the device is lost, stolen, or damaged as a result of irresponsible behavior, the parent may be responsible for the replacement cost, Chromebook: $250.00, iPad: $250.00, MacBook: $500.00 and loss of take-home device privileges.

If the device is damaged, the user may be assessed a $50.00 (MacBook) or $25.00 (Chromebook and iPad) deductible for the repair and/or replacement of the device. Refer to Table of Estimated Repair Pricing for Deductibles on page 7 of Technology Handbook.

In the event a device is lost, a police report must be filed. The MCS, in conjunction and with police or sheriff, may deploy location software which may aid authorities in recovering the device. It is imperative that a lost or stolen device must be reported immediately. If stolen/lost device is not reported within 5 calendar days to MCS personnel, parent/guardian will be responsible for $150.00 (MacBook) or $50.00 (Chromebook and iPad) replacement cost.

Students who leave the District during the school year must return the device, along with any other issued accessories, at the time they leave the District. The device and all accessories should be returned to the school administrator. Any fees collected as a part of this initiative will not be refunded.

**Repossession**
If the user does not fully comply with all terms of this Agreement and the MCS Student Technology Handbook, including the timely return of the property, MCS shall be entitled to declare the user in default and come to the user's place of residence, or other location of the property, to take possession of the property.

**Terms of Agreement**
The user's right to use and possession of the property terminates not later than the last day of the school year unless earlier terminated by MCS or upon withdrawal from MCS.

**Unlawful Appropriation**
Failure to timely return the property and the continued use of it for non-school purposes without the District's consent may be considered unlawful appropriation of the District's property.

# Fees for Device Use

## Use and Maintenance Fees

- Parents/guardians shall pay a non-refundable annual usage fee plus deductibles per damage incident. Annual usage fee: MacBook - $50.00, Chromebook and iPad - $25.00
- District may prorate annual usage fee in the even of casualty or unforeseeable occurrence beyond District control.
- The deductible is by incident (i.e. 1st damage, 2nd damage) AND by incident type (i.e. cracked glass, broken LCD, bent frame, etc.).
- If the device is lost, stolen, or totally damaged as a result of irresponsible behavior, the parent may be responsible for the replacement cost. A police/sheriff report will be required for all stolen devices.
- District may disable the device remotely to protect the device and/or data on the device.
- Seniors must clear all records and pay all fees before they shall be allowed to participate in commencement exercises.

## Damaged Device

Any damage must be reported to school authorities immediately. Power adapters must be returned or paid in full. If a device is damaged and needs repair, the student will be assigned a loaner until the original device is returned. Once the damaged device is repaired, the original device will be returned to the student and any fees must be paid within (7) seven business days.

## Occurrence Deductibles:

- First damage occurrence: Chromebook: Covered by usage fee / iPad: $25.00 / MacBook: $50.00 deductible.
- Second damage occurrence: : Chromebook: $25.00 / iPad: $25.00 / MacBook: $50.00 plus the cost to repair the device or fair market value and possible loss of device take-home privileges.
- Third damage occurrence: Chromebook/iPad: $50.00 plus damage fee and loss of take-home device privileges. MacBook: $100.00 plus cost to repair the device or fair market value and loss of take-home device privileges.

Table of Estimated Repair Pricing for Deductibles

| Loss, Deliberate Damage or Neglect Estimated Repair/Replacement | MacBook | iPad | Chromebook |
|---|---|---|---|
| Broken Screen | $150.00 | $75.00 | $75.00 |
| Broken Keyboard | $150.00 | N/A | $75.00 |
| Power Adapter + Cord | $60.00 | $40.00 | $30.00 |
| Power Adapter | $40.00 | $20.00 | $15.00 |
| Power Cord | $20.00 | $20.00 | $15.00 |
| Liquid damage to Device | $150.00 | $75.00 | $75.00 |
| District Assigned Case | $25.00 | $25.00 | $25.00 |
| Trackpad Damage | $150.00 | N/A | $75.00 |
| Severe Damaged Corner | $150.00 | $75.00 | $75.00 |
| Writing, Drawing, Stickers, and Labels attached | $50.00 | $25.00 | $25.00 |

## Handling and Care of the Device

- Keep the device in the district-issued or approved sleeve and case, if applicable.
- Keep device free of any writing, drawing, stickers, or labels that are not applied by MCS.
- Use the device on a flat, stable surface.
- Do not place books on the device.
- Do not have food or drinks around the device.
- Wipe surfaces with a clean, dry soft cloth.
- Avoid touching the screen with pens or pencils.
- Do not leave the device exposed to direct sunlight or near any heat or moisture sources for extended periods of time.

**Power Management**

- It is the user's responsibility to recharge the device's battery, so it is fully charged by the start of the next school day.
- Device with no battery life must be charged in the classroom. The student forfeits use of the device for the entire time it takes to charge the device.
- All class work missed because of uncharged batteries must be made up on a student's own time.
- The device must remain on (awake or sleep mode) at school at all times, with no exceptions.

**Transport**

- Transport device in its protective case. If protective case is removed, the district personnel has the rights to obtain device until protective case is returned or new case is purchased.
- Do not leave the device in a vehicle for extended periods of time or overnight.
- Do not leave the device in visible sight when left in a vehicle.

**Monitoring and Supervision**

- Do not leave the device unattended in an unlocked classroom or during an extracurricular activity.
- Do not lend the device to a classmate, friend, or family member.
- Any attempt to "jailbreak" or remove the MCS profile could result in disciplinary action, including suspension.
- The user is responsible for the safety and security of the device.

## ACCEPTABLE USE POLICY AND PROCEDURES

The District recognizes the value of computer and other electronic resources to improve student learning, teaching, instruction, research and communication to enhance the administration and operation of its schools. To this end, the MCS provides Intranet (internal) and Internet (external) connections for staff, students, and faculty. MCS encourages the responsible use of computers, computer networks, including the Internet, e-mail, and other electronic resources in support of the mission and goals of the MCS and its schools.

In order to access District services such as the Intranet and Internet via the District Network, each user must sign a Statement of Assurance (SOA) to acknowledge agreement with this Acceptable Use Policy (AUP) stating that he/she is has read and acknowledges agreement with all the sections below.

The operation of the MCS network is guided by policy or policies set forth by the Board of Education of Madison County School District, District administration, the Mississippi Department of Education, and/or all applicable local, state and federal Laws. This AUP does not list every applicable policy or law, but sets forth some specific policies particular to MCS.

### MONITORING OF NETWORK USE

All data transferred and /or transmitted over the MCS network can be monitored and recorded at any time. All data transferred or transmitted over the network can be tracked and identified, and originating users can be held liable if their use of the network violates any established policy, regulation, or law. Any data stored on District-owned equipment may be archived and preserved by the District for an indefinite period. Such data includes, but is not limited, to email, text documents, digital photographs, music and other digital or electronic files.

### SCHOOL DISTRICT OWNERSHIP

All data transferred over the District network or stored on any District-owned equipment/media is the property of MCS.

### CONSEQUENCES OF POLICY VIOLATION(S)

The use of the District Network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. Any student or District employee, including contract services (outside parties), who violate any policy, regulation, or law regarding use of the District Network will be identified and corrective and /or punitive actions will be taken.

All users of the MCS network are charged with reporting violations or misconduct to their teachers, supervisors, or the Network administrator. Users who fail to report violations are subject to the same disciplinary actions as those who violate the policy.

Violations of these procedures may result in, but is not limited to, loss of access privileges, disciplinary action by the District, and / or involvement of law enforcement authorities.

### DISCLAIMER OF LIABILITY

MCS disclaims all liability for the content of materials to which a student or employee may have access on the Internet and for any harm or damages suffered as a result of the student or employee member's

Internet use. Because the Internet and e-mail is an unregulated, worldwide vehicle for communication, information available to employees and students is impossible to control. Therefore, MCS shall not be responsible for:

- Any damages a student or employee may suffer, including, but not limited to, loss of data or interruption of services,
- For the accuracy or quality of information obtained from or stored on any of its network or client systems,
- Financial obligations arising through the unauthorized use of the systems,
- Theft, loss or damage to personal electronic devices,
- Any actions or obligations of a student or employee while accessing the Internet outside the public school system for any purpose.

While MCS takes steps to protect users from inappropriate material, to intercept unlawful and malicious actions from affection users, to safeguard users, no system is perfect. Those risks must be recognized and accepted by users who sign the AUP SOA.

**FILTERING**

MCS uses an aggressive Content Filter and SPAM filter. MCS complies with the regulations of CIPA, the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)], to provide Internet content filtering services for staff and students. Filtering services are a means of protection from objectionable sites but cannot provide a 100% protection. Therefore, MCS provides no guarantees but will attempt to protect employees and students from accessing such objectionable Internet sites. In the event that inappropriate material is accessible, MCS will not be held liable.

**EMAIL AND ELECTRONIC DOCUMENT RETENTION**

All emails and electronic documents created and shared with others inside or outside the District in conducting District business should be saved in user-designated folders on the user's computer.

All District employee email will be archived for a minimum of one year.

All District employees and students in Grades 6-12 will be issued a District email account. Any official communications, e.g. teacher to parent, teacher to student, student to teacher, staff to staff, must be via the District's madison-schools.com email system. This includes, but is not limited to, teachers who guide extracurricular activities such as clubs, choirs, bands, athletic teams, etc.

District employees, who generate newsletters, memoranda, slide shows, graphics, etc. with their workstations, devices, or other district equipment, should organize their computer's workspace (storage) using folders to store electronic documentation.

Use of "Internet Mail" by students and employees, such as Yahoo mail, Gmail, and POP3 accounts provided by their "home" Internet service providers are allowed at this time.

**PROHIBITED ACTIONS**

The following actions on the District Network are specifically prohibited, and this list is not all inclusive but by way of example:

- Installing software, software application, utility, plug-in or other such operations without the approval of the Technology office;

- Creating, downloading, storing, sending, or displaying offensive messages or pictures including but not limited to pornographic or other sexually explicit material;
- Inserting, using, or attaching non-approved disks, CD-ROMs, or other media storage devices into or with computers;
- Using obscene, profane, or vulgar language;
- Harassing, insulting, intimidating, or attacking others;
- Giving out personal information about another person such as home address or phone number
- Engaging in any practice(s) that threaten the network and other technological tools;
- Violating copyright laws;
- Downloading entertainment/music/video/movie software or other files for transfer to a user's home computer, other personal computer, DVD, or any music/movie device. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the MCS. Software, files, and/or licenses owned by MCS cannot be transferred to staff or student personal or home computers.
- Using the password of others to access the network or any other electronic information or telecommunication services;
- Accessing the documents, files, folders, or directories of others without permission from the owner of the files;
- Using the network and telecommunication services for commercial promotion, product endorsement, or advertisement not previously approved by the MCS School Board
- Using the network, electronic information, computer-driven software and telecommunication services for personal gain or convenience;
- Conducting business other than that deemed academic in nature over the network;
- Misusing the resources of the district's network, electronic information, computer-driven software, or telecommunications service equipment and supplies;
- Promoting causes that are religious in nature, with no apparent educational or instructional value; and/or
- Violating this or other procedures and guidelines establish and set forth by MCS Technology Office.
- Attempt to bypass network controls and filters.

**STIPULATIONS FOR WEBSITE USE AS DISTRICT REPRESENTATIVES**

Use of Non-District web sites to present information, classrooms, clubs, or any other officially sponsored activities of the MCS is prohibited. Any sanctioned activity must be hosted on the District website, (http://www.madison-schools.com). All web publications will abide by the Family Education Rights and Privacy Act (FERPA) for the dissemination of student information.

Current teacher or organization web sites operating outside the MCS's website as of July 1, 2008, will be granted exception from this new procedure. However, a statement of disclaimer must be posted at the school's website and a section under the name of each teacher or organization that has an external web site.

The disclaimer must read, "DISCLAIMER; you are now leaving the Madison County Schools Web Site. The District does not endorse and assumes no responsibility for content or control of the web site(s) to which you are about to proceed. The link provided at this page is a courtesy service. Responsibility of external web site control and content rest solely on the author(s) or manager(s) or Webmaster(s) of such web site(s) and not with the District."

At the external teacher or organization web site, another disclaimer should be posted, “As (a) representative(s) of the Madison County School District, responsibility of external web site control and content rest solely on the author(s) or manager(s) or webmaster(s) of this web site(s) and not with the district. MCS does not endorse this web site for school, academic, business, or any other purposes.” Personal electronic devices used on the district network should have anti-virus and spy ware software installed when applicable.

# Madison County Schools

## Device User Agreement

**As a borrower of an MCS device:**

- I have signed and will follow the policies established in the MCS Student Technology Handbook.
- I will follow the guidelines listed below for proper care of the device.
- I will report to school authorities any problems/issues I discover while using the device.
- I understand that resetting the device to factory settings may occur as a result of any repairs or modifications on the device, and this reset may result in the loss of data.
- I understand that it is my responsibility to turn in my device for periodic updates throughout the school year.
- I understand that the primary use of the device is as an instructional tool.

**Guidelines for Proper Care of the Device**

1. I shall not loan the device to anyone.
2. I will not remove labels, stickers, or screen protectors already placed on the device by the technology department.
3. I will not write on or place any labels or stickers on the device.
4. I shall give proper and due care to the device at all times, including but not limited to the following:
    a. Keeping food and drink away from the device.
    b. Not exposing the device to extreme heat or cold.
    c. Not attempting to repair a damaged or malfunctioning device.
    d. Not upgrading the device operating system unless directed by District IT staff.
    e. Using the appropriate device A/C adapter to charge the device.
5. I shall provide proper security for the device at all times including, but not limited to, the following:
    a. Not leaving the device unattended in an unlocked classroom or extra-curricular activity.
    b. Not leaving the device in an unlocked vehicle.

**Device Management**

1. I shall not sync the device to personal or school computer.
2. District purchased software will be installed on to student device.
3. To protect the student and the district from loss of a device, the Computrace service must remain on at all times.
4. The District will monitor any and all usage of the hotspots, including but not limited to the types of data used. Any data usage through the hotspot (including by personal devices) may be monitored by the District, and no data that passes through the hotspot is private.
5. The District may, at its discretion, limit the speed or amount of data available through the hotspot.
6. The District may also turn off the hotspot, disconnect service to the hotspot, or require return of the hotspot, at its sole discretion.