MCSS

Madison County School System

Acceptable Use Agreement

2023-2024

Madison County Board of Education, Approved March 23, 2023

MCSS
Madison County School System

MCSS Acceptable Use Agreement

MCBOE Approved 03.23.2023

Responsible Use of Technology

The Madison County School System provides its students and staff access to a variety of technological resources, including digital devices and Internet connectivity. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. As the technological environment is large and varied, the use of technology by students and employees must be legal and ethical; and it should be consistent with the educational vision, mission, and goals of the Madison County Board of Education.

Through the school district's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information. The district intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. Accordingly, the MCSS Acceptable Use Agreement (AUA) will govern student and employee use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections; the resources, tools, and learning environments made available by or on the networks; and all devices that connect to those networks.

The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of the Madison County School System. The use of any and all MCSS technology resources is a privilege and not a right.

Each user is expected to abide by the generally accepted rules of network etiquette, the provisions in this Parent-Student Handbook, and the Student Code of Conduct. Violations of these provisions, or applicable laws and regulations, may result in the loss of computer services, disciplinary action to include termination of employment and/or appropriate legal action, and/or assessment of the cost of damages to hardware/software.

Privacy

No right to privacy exists in the use of MCSS technological resources. Users should not assume that files or communications accessed, downloaded, created, or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private.

School district administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept email messages to maintain system integrity and to ensure compliance with policy and applicable laws and regulations. School district personnel shall monitor the online activities of individuals who access the Internet via a school-issued account. Under certain circumstances, the district may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the Board, as a response to a public records request, or as evidence of illegal activity in a criminal investigation.

Students shall not reveal or post any personal or contact information about themselves or other people on websites and/or social media sites while utilizing district technology resources. Personal information includes, but is not limited to, names, addresses, telephone numbers, photos or likenesses, videos, ages, dates of birth, grade levels, social security numbers, or any other information by which a person might be identified.

Any online message, comment, image, or anything else that causes a student to be concerned for his/her personal safety should be brought to an adult's attention. Students should immediately bring any threatening or unwelcome communications to the attention of school personnel.

Access

Access to the MCSS network and communication system will be governed as follows:

- All users will be required to acknowledge their receipt and understanding of the responsible use guidelines as published in the MCSS Parent-Student Handbook, Student Code of Conduct, and the MCBOE Policy.
- Access to the district's electronic communication system, including the Internet, shall be made available to students primarily for instructional and administrative purposes.
- MCSS passwords for all staff and students will be changed routinely and two-factor authentication may be implemented.

Employees and students authorized to access the MCSS network are assigned login credentials. These login user names and passwords must be kept confidential to ensure system security.

- Do not write down or post your MCSS password.

- Do not share your MCSS password
- Do not log into an account for anyone other than yourself. This includes logging into an account for a substitute teacher or a student.
- Do not connect or install any technology hardware or software, components, or equipment to MCSS devices. Contact IT for network and equipment connection questions.

Electronic Mail (Email)

The Madison County School System provides access to electronic mail for all employees and for specific and selected student use. Such access is for his/her use in any educational and instructional business that they may conduct. Limited personal use of electronic mail is permitted as long as it does not violate MCBOE policy and/or adversely affect others.

- Electronic mail shall not be used to promote political, religious, and/or personal gains.
- The Board cannot guarantee the privacy, security, or confidentiality of any information sent or received via electronic mail.
- Network administrators can review e-mail, file folders, and communications to maintain system integrity and ensure that users are using the system responsibly.
- A confidentiality statement in email messages does not guarantee any legal protection, therefore, they should not be added to any MCSS emails.

Internet Safety

The Madison County School System, either by itself or in combination with the Internet Provider, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors.

The School will also monitor the online activities of students through direct observation or technological means. Any time a student is logged into Google Chrome while on their school-owned account, whether on a school-issued or personal device, they may be monitored to ensure that students are not accessing such depictions or any other material that is inappropriate for minors. This monitoring can include web searches, social media, videos, or Google products.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age seventeen (17) and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h] [7]), as meaning any picture, image, graphic image file, or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors
- An actual or simulated sexual act or sexual contact
- An actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors

Data Security

The Madison County School System takes seriously its obligations to secure data systems and protect the privacy of students and employees. Strict processes help safeguard the confidentiality and security of the data.

- Employees may use only accounts, files, software, applications and/or other technology resources that are assigned to, provided, or approved Data Governance Committee.
- **Staff and students should not have any expectation that their usage of such resources is private.** Reasonable efforts will be taken to maintain security of technology resources, but MCSS cannot ensure that such security will not be penetrated or breached and cannot assume any liability arising out of any such penetration or breach of security.
- Employees are prohibited from emailing outside the school system or storing/saving on external storage devices or portable devices that do not remain on within official district systems, electronic copies of student or staff personal information. This information includes, but is not limited to data containing social security numbers, information protected by FERPA, and any other sensitive and/or protected information. In the event that this type of information is stored on a portable or external device and said device is lost or stolen or if the security of this data is believed to have been breached in any way, the Director of IT should be notified immediately.
- All electronic content stored on any external storage medium or personal off-site storage location that is brought to or accessed from an MCSS is subject to all Board policies and guidelines, as well as local, state, and federal laws.
- Because communications on the internet are public in nature, all staff and students should be careful to maintain appropriate and responsible communications.
- Staff and students are encouraged to avoid storing personal and/or private information on the district and/or school's technology resources. Users must be careful of Social engineering, in the context of information security, refers to the psychological

manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. Users are still responsible for any type of data breach they create regardless of falling prey to social engineering.

- Staff and students must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside the Madison County School System. Any such unauthorized usage shall be reported immediately to the local school Director of Information Technology.
- All staff and students shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical security measures.
- Permission for publishing employee photographs on the MCSS website is assumed unless the employee specifies otherwise in writing to his or her direct supervisor.
- Staff and students may not attempt to log into the network or application using any account and/or password other than the login(s) assigned to him/her. Individuals may not allow someone to use his/her network account and/or password to access the network, email, specific software packages, or the Internet.
- Staff and students are expected to follow all local, state and federal laws and system policy regarding the protection of student and staff confidential data.
- MCSS assumes no responsibility for any unauthorized charges made by students on MCSS devices, internet services, and/or network included but not limited to credit card charges, long distance phone charges, equipment and line costs, or for any illegal use such as copyright violations.

Personal Technology Devices

A personal technology device (PTD) is a portable Internet-accessing device that is not the property of the school district that can be used to transmit communications by voice, written characters, words, or images; share information; record sounds; process words; and/or capture images, such as a laptop computer, tablet, smartphone, smartwatch, cell phone, or any other electronic communication device.

A student may possess and use a PTD on school property, however, the use of such devices is at the discretion of the principal at each school. Under no circumstances may students possess or use a PTD during any state assessment or secure exam.

Possession of a PTD by a student is a privilege that may be revoked for violations of the Code of Student Conduct. Violations may result in the confiscation of the PTD (to be returned only to a parent) and/or other disciplinary actions

The school district is not responsible for theft, loss, or damage to PTDs or other electronic devices brought onto school district property. Students permitted to use PTDs during the school day must follow Board policy concerning Internet safety and use of technology.

Cyberbullying

Cyberbullying will not be tolerated. Engaging in these behaviors may result in disciplinary actions and/or loss of privileges. Examples of cyberbullying include but are not limited to:

- Harassment
- Intimidation
- Threats
- Impersonation
- Insults
- Displaying offensive photos/images/videos
- Lewd behavior

Refer to the MCSS Student Code of Conduct
Refer to the FTC Online Security website for more information

Copyright & Plagiarism

All users are expected to abide by copyright laws and to follow the *Fair Use Guidelines for Educational Multimedia*. If students do not know if the use of online material is legal or ethical, ask teachers or administrators for guidance.

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Refer to the Fair Use Guidelines for Education Multimedia
For more information visit NASSP
Copyright Basics
TEACH Act 2002

MCSS Property

Students and their parents are personally responsible for the proper care, use, and handling of the assigned devices. Students are responsible for promptly submitting damaged, broken, or non-working devices to the designated school personnel for repair.

The parents of a student who is found responsible for the loss, destruction, breakage, or damage of school equipment (such as, but not limited to, the device, batteries, cords, and chargers) may be required to pay for the replacement equipment. Replacement or repair cost depends on the severity of the damage.

If a student's device is lost or stolen, the student and/or parent are responsible for obtaining a police report within 24 hours of discovery of the loss/theft, immediately providing the school with documentation of the report, and cooperating fully with any subsequent investigation.

The MCSS and manufacturer's identification tags will not be tampered with or removed. No other stickers, ink, or any decorative items may be added to a student's (or staff) assigned equipment (such as, but not limited to, the device, batteries, cords, and chargers).

Students and parents shall address all concerns regarding the use of the technology to the supervising teacher(s) and/or the school administrative staff.

MCSS
Madison County School System

MCSS Acceptable Use Agreement

MCBOE Approved 03.23.2023

Responsible Use of Technology

The Madison County School System provides its students and staff access to a variety of technological resources, including digital devices and Internet connectivity. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. As the technological environment is large and varied, the use of technology by students and employees must be legal and ethical; and it should be consistent with the educational vision, mission, and goals of the Madison County Board of Education.

Through the school district's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information. The district intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. Accordingly, the MCSS Acceptable Use Agreement (AUA) will govern student and employee use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections; the resources, tools, and learning environments made available by or on the networks; and all devices that connect to those networks.

The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of the Madison County School System. The use of any and all MCSS technology resources is a privilege and not a right.

Each user is expected to abide by the generally accepted rules of network etiquette, the provisions in this Parent-Student Handbook, and the Student Code of Conduct. Violations of these provisions, or applicable laws and regulations, may result in the loss of computer services, disciplinary action to include termination of employment and/or appropriate legal action, and/or assessment of the cost of damages to hardware/software.

Privacy

No right to privacy exists in the use of MCSS technological resources. Users should not assume that files or communications accessed, downloaded, created, or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private.

School district administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept email messages to maintain system integrity and to ensure compliance with policy and applicable laws and regulations. School district personnel shall monitor the online activities of individuals who access the Internet via a school-issued account. Under certain circumstances, the district may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the Board, as a response to a public records request, or as evidence of illegal activity in a criminal investigation.

Students shall not reveal or post any personal or contact information about themselves or other people on websites and/or social media sites while utilizing district technology resources. Personal information includes, but is not limited to, names, addresses, telephone numbers, photos or likenesses, videos, ages, dates of birth, grade levels, social security numbers, or any other information by which a person might be identified.

Any online message, comment, image, or anything else that causes a student to be concerned for his/her personal safety should be brought to an adult's attention. Students should immediately bring any threatening or unwelcome communications to the attention of school personnel.

Access

Access to the MCSS network and communication system will be governed as follows:

- All users will be required to acknowledge their receipt and understanding of the responsible use guidelines as published in the MCSS Parent-Student Handbook, Student Code of Conduct, and the MCBOE Policy.
- Access to the district's electronic communication system, including the Internet, shall be made available to students primarily for instructional and administrative purposes.
- MCSS passwords for all staff and students will be changed routinely and two-factor authentication may be implemented.

Employees and students authorized to access the MCSS network are assigned login credentials. These login user names and passwords must be kept confidential to ensure system security.

- Do not write down or post your MCSS password.

- Do not share your MCSS password
- Do not log into an account for anyone other than yourself. This includes logging into an account for a substitute teacher or a student.
- Do not connect or install any technology hardware or software, components, or equipment to MCSS devices. Contact IT for network and equipment connection questions.

Electronic Mail (Email)

The Madison County School System provides access to electronic mail for all employees and for specific and selected student use. Such access is for his/her use in any educational and instructional business that they may conduct. Limited personal use of electronic mail is permitted as long as it does not violate MCBOE policy and/or adversely affect others.

- Electronic mail shall not be used to promote political, religious, and/or personal gains.
- The Board cannot guarantee the privacy, security, or confidentiality of any information sent or received via electronic mail.
- Network administrators can review e-mail, file folders, and communications to maintain system integrity and ensure that users are using the system responsibly.
- A confidentiality statement in email messages does not guarantee any legal protection, therefore, they should not be added to any MCSS emails.

Internet Safety

The Madison County School System, either by itself or in combination with the Internet Provider, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors.

The School will also monitor the online activities of students through direct observation or technological means. Any time a student is logged into Google Chrome while on their school-owned account, whether on a school-issued or personal device, they may be monitored to ensure that students are not accessing such depictions or any other material that is inappropriate for minors. This monitoring can include web searches, social media, videos, or Google products.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age seventeen (17) and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h] [7]), as meaning any picture, image, graphic image file, or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors
- An actual or simulated sexual act or sexual contact
- An actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors

Data Security

The Madison County School System takes seriously its obligations to secure data systems and protect the privacy of students and employees. Strict processes help safeguard the confidentiality and security of the data.

- Employees may use only accounts, files, software, applications and/or other technology resources that are assigned to, provided, or approved Data Governance Committee.
- **Staff and students should not have any expectation that their usage of such resources is private.** Reasonable efforts will be taken to maintain security of technology resources, but MCSS cannot ensure that such security will not be penetrated or breached and cannot assume any liability arising out of any such penetration or breach of security.
- Employees are prohibited from emailing outside the school system or storing/saving on external storage devices or portable devices that do not remain on within official district systems, electronic copies of student or staff personal information. This information includes, but is not limited to data containing social security numbers, information protected by FERPA, and any other sensitive and/or protected information. In the event that this type of information is stored on a portable or external device and said device is lost or stolen or if the security of this data is believed to have been breached in any way, the Director of IT should be notified immediately.
- All electronic content stored on any external storage medium or personal off-site storage location that is brought to or accessed from an MCSS is subject to all Board policies and guidelines, as well as local, state, and federal laws.
- Because communications on the internet are public in nature, all staff and students should be careful to maintain appropriate and responsible communications.
- Staff and students are encouraged to avoid storing personal and/or private information on the district and/or school's technology resources. Users must be careful of Social engineering, in the context of information security, refers to the psychological

manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. Users are still responsible for any type of data breach they create regardless of falling prey to social engineering.

- Staff and students must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside the Madison County School System. Any such unauthorized usage shall be reported immediately to the local school Director of Information Technology.
- All staff and students shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical security measures.
- Permission for publishing employee photographs on the MCSS website is assumed unless the employee specifies otherwise in writing to his or her direct supervisor.
- Staff and students may not attempt to log into the network or application using any account and/or password other than the login(s) assigned to him/her. Individuals may not allow someone to use his/her network account and/or password to access the network, email, specific software packages, or the Internet.
- Staff and students are expected to follow all local, state and federal laws and system policy regarding the protection of student and staff confidential data.
- MCSS assumes no responsibility for any unauthorized charges made by students on MCSS devices, internet services, and/or network included but not limited to credit card charges, long distance phone charges, equipment and line costs, or for any illegal use such as copyright violations.

Personal Technology Devices

A personal technology device (PTD) is a portable Internet-accessing device that is not the property of the school district that can be used to transmit communications by voice, written characters, words, or images; share information; record sounds; process words; and/or capture images, such as a laptop computer, tablet, smartphone, smartwatch, cell phone, or any other electronic communication device.

A student may possess and use a PTD on school property, however, the use of such devices is at the discretion of the principal at each school. Under no circumstances may students possess or use a PTD during any state assessment or secure exam.

Possession of a PTD by a student is a privilege that may be revoked for violations of the Code of Student Conduct. Violations may result in the confiscation of the PTD (to be returned only to a parent) and/or other disciplinary actions

The school district is not responsible for theft, loss, or damage to PTDs or other electronic devices brought onto school district property. Students permitted to use PTDs during the school day must follow Board policy concerning Internet safety and use of technology.

Cyberbullying

Cyberbullying will not be tolerated. Engaging in these behaviors may result in disciplinary actions and/or loss of privileges. Examples of cyberbullying include but are not limited to:

- Harassment
- Intimidation
- Threats
- Impersonation
- Insults
- Displaying offensive photos/images/videos
- Lewd behavior

Refer to the MCSS Student Code of Conduct
Refer to the FTC Online Security website for more information

Copyright & Plagiarism

All users are expected to abide by copyright laws and to follow the *Fair Use Guidelines for Educational Multimedia*. If students do not know if the use of online material is legal or ethical, ask teachers or administrators for guidance.

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Refer to the Fair Use Guidelines for Education Multimedia
For more information visit NASSP
Copyright Basics
TEACH Act 2002

MCSS Property

Students and their parents are personally responsible for the proper care, use, and handling of the assigned devices. Students are responsible for promptly submitting damaged, broken, or non-working devices to the designated school personnel for repair.

The parents of a student who is found responsible for the loss, destruction, breakage, or damage of school equipment (such as, but not limited to, the device, batteries, cords, and chargers) may be required to pay for the replacement equipment. Replacement or repair cost depends on the severity of the damage.

If a student's device is lost or stolen, the student and/or parent are responsible for obtaining a police report within 24 hours of discovery of the loss/theft, immediately providing the school with documentation of the report, and cooperating fully with any subsequent investigation.

The MCSS and manufacturer's identification tags will not be tampered with or removed. No other stickers, ink, or any decorative items may be added to a student's (or staff) assigned equipment (such as, but not limited to, the device, batteries, cords, and chargers).

Students and parents shall address all concerns regarding the use of the technology to the supervising teacher(s) and/or the school administrative staff.