MONTROSE R-XIV SCHOOL

2020-2021

Technology Handbook

Approved: August 3, 2020

Table of Contents

GENERAL INFORMATION

Montrose R-XIV School District laptop technology devices, hereafter referred to as "devices," are the property of the District. Devices are on loan to students, and must be used in accordance with Board policies and procedures, as summarized in this technology handbook, and any applicable state and federal laws. Use of devices, as well as access to the District's network, the internet, and email are a privilege and not a right. Technology is provided for educational purposes only, and is intended to support the learning objectives of the District.

The procedures and information in this handbook apply to all student device use in the District, including any other device considered by the administration to fall under the guidelines of this handbook. Teachers may set additional requirements for use in their individual classrooms.

DEVICE DEPOSIT/REPAIR/REPLACEMENT INFORMATION FOR PARENTS/ GUARDIANS:

Parents/ guardians are responsible for paying the costs for device repairs. Repair bills are to be paid to the Montrose R-XIV Central Office. ANY lost device requires the student's parent/ guardian to report the situation to the District and file a police report. If the device is not recovered in good working order as when issued to the student, the student/parent will be responsible for paying the replacement cost.

LAPTOP IDENTIFICATION:

Each device has a unique ID and is assigned to an individual student. Each device can be identified by the District in the following ways:

- Record of the device's Serial Number matched to individual student names.
- Record of the mac address of the device.
- District label with unique ID on each device.

Students must never attempt to hide or take off device IDs. Please inform the central office of damaged labels and new ones will be provided.

RETURNING DEVICES:

Students must return their devices and all accessories to the District during the last week of school each year, or when directed to do so by a teacher or administrator.

Students who transfer out of the District must return their device(s) and accessories before records are 100% cleared for transfer. Students who withdraw, are suspended or expelled, or terminate enrollment in the District for any reason must return devices and accessories on the date of termination / withdrawal.

RULES FOR DEVICE USAGE

Devices are to be used in the classroom and home for student academic and educational purposes, only. Devices are intended for use at school each day. In addition to teacher expectations for device use, school messages, announcements, calendars, schedules, and the

Parent Portal may be accessed using devices. Students must bring their devices to all classes, unless specifically instructed not to do so by an individual teacher.

STUDENTS MUST:

1. Never "swap" or share their device(s) with another student, unless directed by a teacher do so for a supervised classroom activity.
2. Maintain possession of their devices at all times, or ensure they are secured in a designated classroom / location at all times.
3. Never share passwords with another student. Passwords are to remain strictly confidential. If you suspect someone knows your password, see the central office to have it changed.

CHARGING YOUR DEVICE:

Students who take their devices home are responsible for bringing their device fully charged to school each day. Students need to charge their devices each evening.
Administration will have plans in place to assist students in this process, when needed.
Repeated violations will result in the student losing the privilege to use the device at home and/or other disciplinary measures.

HOME INTERNET ACCESS:

Students are allowed to set up home wireless networks on their devices.

IF DEVICE IS LEFT AT HOME:

If a student leaves his/ her device at home, they are still responsible for getting class work completed. If a student repeatedly leaves his/ her device at home, he/ she will lose privileges to use the device at home. In such cases, the student will be required to return the device to the appropriate charging area each day and leave the device at school.

IF DEVICE IS LEFT I N AN UNSECURED AREA:

Under NO circumstances should devices be left in unsecured / unsupervised areas. Unsecured areas are all public use areas of the school, including but not limited to: the stage, bleachers, lunchroom, computer lab, locker room, library, unlocked classrooms, dressing rooms, hallways, and restrooms. Devices left in unsecured and unsupervised areas are in extreme danger of being stolen.
If a student is participating in an activity that is not conducive to having the device (i.e., field trips, assemblies, sports, etc.), they are required to secure the device in the charging cart or locked in their hallway locker. SCHOOL DEVICES ARE NEVER TO BE IN LOCKER ROOMS. Students in PE must leave their devices in their locked hallway lockers (ensuring nothing is on top of them). Devices found in unsecured areas will be taken to the office and students may be required to complete alternate assignments due to temporary loss of device. Repeated offenses will result in disciplinary action.

NETWORK CONNECTIVITY:

The District makes no guarantees that their network will be up and running 100% of the time. In the rare case that the network is down, the District will not be responsible for lost or missing data.

PERIODIC DEVICE INSPECTION:

District staff will periodically check devices for unauthorized materials or activities.

RULES FOR USI NG DEVICES AT HOME:

1. Students must have written permission of their parents/ guardians on file, and their technology user fee deposit must be paid before they will be allowed to take devices home.
2. When at home, devices must always be used under the direct supervision of an adult in a common family location (i.e., kitchen, living room).
3. Devices must not be placed on or under soft items such as pillows, chairs, sofa cushions, or blankets. Doing so will cause devices to overheat and can result in permanent damage.
4. If a device is lost or stolen, parents/ guardians should immediately report the loss or theft to the school at 660-693-4812.
5. If the device is damaged or not working properly, it must be turned into the office. Parents/ guardians are responsible for paying the costs for device repairs. The District will then send the broken device for repair or replacement. Parents/ guardians are not authorized to attempt repairs themselves or to contract with any other individual or business for the repair of a device. Such action will void the warranty.

SAVING TO THE / HOME DIRECTORY:

Students may save work directly on the device. However, it is recommended that students save their work on a flash drive and /or apps. Storage space will be available but it will NOT be backed up in case of re-imaging. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Flash drives and other memory/storage devices used in school devices are subject to search with reasonable suspicion that prohibited / illegal activities/ materials are present, in accordance with the law.

SCREENSAVERS AND BACKGROUNDS:

Inappropriate media may not be used as a screensaver or background photo. Inappropriate media includes, but is not limited to: Depictions of guns, weapons, pornography, inappropriate language, vulgarity, tobacco, alcohol, drugs, gang-related symbols, or those that are threatening, harassing, or discriminatory against protected classes. Use of such screensavers or backgrounds will result in disciplinary action, when not protected by law.

SOFTWARE AND APPS ON DEVICES:

Originally Installed Software - The software and apps originally installed by the District must remain on the device in usable condition and be easily accessible at all times. From time to

time, the school may add software and apps for use in a particular class. Period device checks will be made to ensure students have not removed any required apps or added apps that are not authorized by the District. Disciplinary measures per the student handbook may be incurred.

Additional Software and Apps - Students are not allowed to load extra software or apps on the devices unless otherwise directed to do so by their teachers or school staff. The District will synchronize the devices so that they contain the necessary apps. Students will not synchronize devices or add apps to devices, including home synching accounts. Disciplinary measures per the student handbook may be incurred.

Procedure for Reloading Software – If technical difficulties occur or unauthorized software or apps are discovered, the device will be restored from backup. The District does not accept responsibility for the loss of any software or documents deleted due to a reformat and reimage. Disciplinary measures per the student handbook may be incurred.

Software Upgrades - Upgrade versions of licensed software and apps are available from time to time. Students may be required to check in their devices for periodic updates and synching.

SOUND, MUSIC, GAMES, CAMERA, AND PROGRAMS:

Sound must be muted at all times unless permission is obtained from the teacher for a specific instructional purpose. Music is allowed on devices only for educational purposes and is only to be used at teacher's discretion. Programs, games, etc. out of compliance with technology regulations that have been saved to memory sticks are not allowable on school devices. Students are not allowed to download or install ANY software, illegal music or movies, or other copyrighted materials. If the device has a camera, no photos or videos are to be taken that are not academic related without prior approval from the principal, and only for those reasons allowable in District policy. All software / apps must be school-approved and installed by a staff member. Data storage will be through apps on devices and email to a server location. Inappropriate usage for purposes in this section will result in disciplinary action.

STUDENT DISCIPLINE:

The discipline policies and procedures outlined in Montrose R-XIV School District Student Handbook address the major and minor offenses related to school technology, both on and off school property. Depending upon the seriousness of each individual offense, students may lose device and / or network privileges, as well as face suspension, expulsion, and even report to law enforcement, where applicable. Please see respective handbooks for more information.

TAKING CARE OF DEVICES:

1. Students will be held responsible for maintaining their devices and keeping them in good working order throughout the school year.
2. Device batteries must be charged at home each night and ready to use each school day, or placed on chargers in stations located at school, for students who do not take devices home.
3. Devices must be returned with only normal wear and no alterations at the end of the school year. Students will be charged replacement fees if devise cases or bags assigned to them are damaged beyond normal wear.

4. Devices must always be within their protective cases/ bags when carried.
5. Cords and cables must be inserted carefully into devices to prevent damage.
6. When transporting devices using backpacks or other similar carrying cases, use extra caution as to avoid potentially causing damage such as a broken screen.
7. Students are not to put labels or stickers on devices.
8. When students are not using their devices, they must be stored in a secure location. Nothing can be placed on top of devices when stored.
9. Devices must not be stored in vehicles at school or home. Devices will be damaged from high temperatures and cold temperatures.
10. If a student needs a secure place to store their device, school staff will provide assistance.
11. Devices that malfunction or are damaged must be reported to the teacher or office immediately.
12. Cost to repair devices and accessories that have been damaged from student misuse, neglect, or intentional damage will be the student's responsibility.
13. 0nly use a clean, soft cloth to wipe the screen; no cleansers of any type.

USING DEVICES FOR INTERNET AND EMAIL:

Students and parents/ guardians understand the District does not have control over information found on the internet. While every attempt is made to block access to inappropriate materials while students are at school, the District is not able to monitor student usage of devices while at home. It is the responsibility of parents/ guardians to supervise the information student's access on the internet while at home.

1. Students must never share personal information about themselves on the internet. This includes a student's name, age, address, phone number, or school name.
2. Parents/ guardians and students are required to read and agree to the District's Parent-Student Acceptable Technology Usage Agreement and sign it prior to receiving their devices.
3. Students must be aware that internet access and email, as well as other media they have accessed, created, or stored on devices is the sole property of the District. The District has the right to review these items for appropriateness and adherence to Board policies, rules, and state/ federal laws, and to revoke students' access to devices at any time and for any reason.

MONTROSE R-XIV SCHOOL DISTRICT
PARENT/STUDENT TECHNOLOGY USAGE AGREEMENT & AUTHORIZATION FOR ELECTRONIC NETWORK ACCESS

Each student and his/ her parents/ guardians must sign the Parent-Student Technology Usage Agreement before being granted access to the District network and given a device. Please read this document carefully before signing.

All use of the internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This Authorization & Agreement does not attempt to state all required or prohibited behaviors of users. However, some specific examples are provided.

Failure of any user to follow the terms of the Authorization for Electronic Network Access & Parent-Student Acceptable Technology User Agreement will result in loss of privileges, disciplinary action, and / or appropriate legal action. The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

TERMS AND CONDITIONS:

Acceptable Use - The use of District technology and electronic resources is a privilege, which may be revoked at any time. Staff and students are only allowed to conduct electronic network-based activities that are classroom or workplace related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses or harmful programs on or through the computer system; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; sending or receiving personal messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.

Students and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students or employees use copyrighted materials without the permission of the copyright holder. The Internet allows users access to a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (E-mail) is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system is designed solely for educational and work related purposes. E-mail files are subject to

be reviewed by District and school personnel. Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.

Students or employees who engage in "hacking" are subject to loss of privileges and District discipline, as well as the enforcement of any District policy, state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, students and employees are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter," which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions.

The District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or other disciplinary action.

Privileges - The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. All staff members and students who receive a password/account code will participate in an orientation or training course regarding proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

- Using the network for any illegal activity, including violation of copyrights or other contracts, or transmitting any material in violation of any State or Federal law;
- Downloading unauthorized software, regardless of whether it is copyrighted or virus-free;
- Hacking or gaining unauthorized access to files, resources, or entities, as well as using non-district proxies;
- Invading the privacy of individuals. This includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, including a photograph or video;
- Using another user's account or password;
- Posting material authored or created by another without his/ her consent;
- Posting anonymous messages;
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive,

harassing, or illegal material; bullying and cyberbullying.

- Using the network while access privileges are suspended or revoked.
- Using electronic media that disrupts the educational process or interferes with the rights of others at any time, either during the school day or after school hours.
- Disrupting or interfering with the system.
- Sending mass electronic mail to multiple users without prior authorization by the appropriate teacher or District administrator.
- Misrepresenting one's identity in electronic communications.
- Engaging in any activity that does not meet the intended purposes of the network, including, but not limited to, illegal, commercial, political, religious, union, or entertainment purposes.

Network Etiquette and Privacy - Students and employees are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

1. System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.
2. System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.
3. System users may not reveal their personal information.
4. System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.
5. System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read Email on a random basis.
6. Use of the District's electronic network for unlawful purposes will not be tolerated and is prohibited.
7. No downloads of music, games, etc. are allowed

Services - While the District is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.

Indemnification - The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees incurred by the District, relating to, or arising out of, any violation of this Authorization & Agreement.

Security - The Board recognizes that security on the District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any

intrusion into secure areas by those not permitted by such privilege creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.
The District does use filtering, blocking or other technology to protect students and staff from accessing Internet sites that contain visual depictions that are obscene, child pornography or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NCIPA).

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet. This includes, but is not limited to, the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the District electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

Data Charges - The District assumes no responsibility for any unauthorized charges or fees, including data charges, long-distance charges, per-minute surcharges, and/or other costs incurred to devices.

Copyright Web Publishing Rules - District policy adheres to copyright law and this must be followed when publishing information on the web, District-sponsored websites, or file servers.

- For each republication of media produced externally (Website, District sponsored website, or file servers), credit indicating the original producer and notification of how and when permission was granted must be visible. When possible, the notice should also include the web address (URL) of the original source.
- The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered the source of permission.

Use of Electronic Mail - The District's electronic mail system and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email where appropriate to aid students and staff members in fulfilling their duties and responsibilities, and as an educational tool. Under the CIPA (Child Internet Protection Act), the District is required to have email filtering in place. This does not assure all spam will be caught, nor does it assure all personal emails from outside district accounts will be delivered.

- The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Email shall be

accessed only by the user to whom the District assigned the account.

- Each user should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an email message which would be inappropriate in a letter or memorandum.
- Electronic messages transmitted via the District's internet server carry with them an identification of the user's internet "domain." This domain name is a registered domain name and thereby identifies the author as being associated with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- Any message received from an unknown sender via the internet should be immediately deleted. If the message is deemed to be of an inappropriate nature, the user needs to notify a District staff member immediately. Downloading any file attached to an internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file transmitted.
- Users are never to reply to or share an email containing personal passwords or sensitive information.
- Use of the District's electronic mail system constitutes consent to these regulations.

Parent/Guardian Consent - Teachers may display a student's work as recognition of student achievement. As a parent/guardian, if you do not want your child's artwork, special projects, or photographs taken by your child or images of your child to be displayed on District-sponsored websites, in printed materials, by video, or by any other method of mass communication, you must notify the building administrator in writing.

Internet Safety - Internet access is limited only to those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users do not engage in "unacceptable uses," as detailed in this Authorization, and otherwise follow this Authorization.

Staff members shall supervise student use of District internet access to ensure the student abides by the Terms and Conditions for Internet Access contained in this Authorization.

Each District device with internet access has a filtering device during school hours that attempts to block most depictions which are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The system administrator and building administrators shall monitor student internet access while at school.
Again: It is the responsibility of parents/ guardians to supervise the information a student is accessing from the internet while at home.

Consequences - The consequences for violating the District's Acceptable Use Policy may include, but are not limited to, one or more of the following:

1. Suspension of District Network privileges;
2. Revocation of Network privileges;

3. Suspension of Internet access;
4. Revocation of Internet access;
5. Suspension of computer access;
6. Revocation of computer access;
7. School suspension;
8. Expulsion; or
9. Student disciplinary action up to and including suspension or expulsion

MONTROSE R-XIV SCHOOL DISTRICT
AUTHORIZATION FOR ELECTRONIC NETWORK
ACCESS & PARENT-STUDENT TECHNOLOGY AGREEMENT AND CONSENT FORM

STUDENT:

I understand that I am responsible for repairs and/or replacement costs for broken or lost devices, chargers, and carrying bags.

I understand broken screens on laptops will incur a full screen replacement cost.

I understand and will abide by this Authorization for Electronic Network Access & Parent-Student Technology User Agreement. I hereby release the Montrose R-XIV School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the internet and assigned devices.

USER NAME: DATE:

USER SIGNATURE:

PARENT / GUARDIAN:

I understand that I am responsible for repairs and/or replacement costs for broken or lost devices, chargers, and carrying bags.

I understand broken screens on laptops will incur a full screen replacement cost.

I have read this Authorization for Electronic Network Access & Parent-Student Technology User Agreement. I understand access is designed for educational purposes and the District has taken precaution to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, representatives, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision, if and when my child's use is not in a school setting, of the device and internet usage. I have discussed the terms of this Authorization with my child, and hereby request that my child be allowed access to the District's network and be issued a school device.

PARENT/GUARDIAN NAME: DATE:

PARENT/GUARDIAN SIGNATURE:

MONTROSE R-XIV SCHOOL DISTRICT

TECHNOLOGY USAGE (STUDENT

USER AGREEMENT)

I have read the Montrose R-XIV School District Technology Usage policy and procedures, and I agree to abide by their provisions. I understand that violation of these provisions may result in disciplinary action taken against me including, but not limited to, suspension or revocation of my access to district technology and suspension or expulsion from school.

I understand that my use of the District's technology resources is not private, and that the District will monitor my electronic communications and all other use of district technology resources and devices. I consent to district interception of, and access to, all of my electronic communications using district resources and devices, as well as downloaded material and all data I store on the district's technology resources. This includes, but is not limited to, deleted files, pursuant to state and federal law, even if the district's technology resources are accessed remotely. I understand that flash drives and other memory/storage devices used in school devices are subject to search with reasonable suspicion that prohibited/illegal activities/materials are present, in accordance with the law.

I understand that this form will be effective for the duration of my attendance in the District unless revoked or changed by the district or me.

USER NAME: DATE:

USER SIGNATURE: