Manor Independent School District

Employee and Student
Acceptable Use Agreement

Please read the following information carefully.
This is a legally binding document for students and employees of Manor Independent School District.

I. OVERVIEW

The Manor Independent School District (MISD) owns and maintains a computer system/network (MISD Network – further defined below). MISD permits students and employees (*herein referred to as MISD Member(s)*) to use and access the MISD Network pursuant to Board Policy CQ (Local) and this Agreement. MISD's goal in allowing such use and access is to promote educational excellence in MISD by providing effective and meaningful classroom instruction and meeting administrative needs while ensuring a safe, ethical and productive electronic learning environment. With this educational opportunity comes responsibility.

Definition of MISD Network: MISD's Network includes all of its computer systems, electronic communication systems and networks of any configuration of hardware and software, including but not limited to the following:

- District provided cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally hosted or externally hosted databases, applications, tools (Internet or District server based);
- District-provided Internet access;
- District-filtered public Wi-Fi;
- Virtual environments; and new technologies as they become available.

Definition of a computer system account: Any login and password information disseminated to MISD Members for the purpose of enrolling into a computer program, whether it is hosted in the District or off-premises. A computer system account includes, but is not limited to: Active Directory (AD), Eduphoria, Skyward, Video Insight Camera systems, login to a non-/domain MISD computer, ID camera software, accounts established to manage online learning programs (such as, but not limited to, Edgenuity, My Virtual Reading Coach, and others).

It will be the MISD Member's responsibility to follow the rules for appropriate and acceptable use.

The Internet is a network of many types of communication and information networks. With access to computers and people all over the world comes the availability of adult content or material that may be considered objectionable and may not be considered to be of educational value in the school setting. In compliance with the Children's Internet Protection Act (CIPA), MISD has installed active content filtering and/or blocking software to restrict access to Internet sites containing material harmful to minors.

While MISD uses filtering technology and protection measures to restrict access to such material, it is not possible to absolutely prevent such access. A MISD Member who incidentally connects to an inappropriate site must immediately disconnect from the site and notify a teacher/administrator. If a MISD Member sees another MISD Member accessing inappropriate sites, he or she should notify a teacher/administrator immediately.

Access to the MISD Network is a privilege, not a right. The efficient operation of the MISD Network relies upon the proper conduct of the MISD Members who must adhere to this Agreement. The matters addressed and set forth in this document are so that MISD Members are aware of the responsibility to follow the rules for appropriate and acceptable access and use that are being made available. In general, this requires efficient, ethical, and legal utilization of the network resources. Noncompliance may result in suspension of access or termination of privileges along with other appropriate disciplinary action consistent with MISD Policies.

All MISD students are required to abide by the Student Code of Conduct. All MISD employees are required to abide by the Code of Ethics and Standard Practices for Texas Educators ("Code of Ethics"), State and Federal law, and MISD Policies. All MISD Members must abide by ethical standards when communicating with other MISD Members, regardless of whether such communication takes place on campus, during instructional time, through the use of the MISD Network or not. Violations of law may result in criminal prosecution as well as disciplinary action by MISD.

MISD will periodically conduct periodic digital drills to all staff in order to review responses from purposefully designed emails of deceptive nature. Staff members that respond to such emails will be required to attend additional training on the proper handling of such emails. Failure to attend such training will result in disciplinary action towards the employee.

II. PHILOSOPHY

a. Risk – Even with filtering, blocking, and anti-virus software, controlling all materials on the MISD Network is impossible. Sites accessible via the MISD Network may contain material that is illegal, defamatory, inaccurate or harmful. With global access to computers and people, a risk exists that MISD Members may access material that may not be of educational value in the school setting.

b. MISD Member Responsibility – MISD Members, like traditional library users, are responsible for their actions in accessing available resources. Should inappropriate materials become available, MISD Members must notify a campus teacher/administrator and/or MISD Network administrator immediately.

III. TERMS AND CONDITIONS

Responsible Use: MISD Network access may be used to improve learning and teaching consistent with the educational goals of MISD. MISD expects legal, ethical, and efficient use of the MISD Network. MISD approved email accounts will be provided for MISD Members based on MISD initiatives. MISD approved social media activities that are educationally related may be used. At no time should personal use of the MISD Network come in conflict or hinder a MISD Member's expected responsibilities.

a. Privilege: Use of a personal MISD Network account is a privilege, not a right.

b. Limited personal use is permitted as long as it:(1) does not impose any tangible cost to MISD, (2) does not unduly burden MISD's technology resources and (3) has no adverse effect on an employee's job performance or on a student's academic performance. MISD will provide a filtered, wireless public network to which staff and students will be able to connect personal computer devices (including but not limited to cell phones, tablets and laptops) for instructional and administrative functions. These personal devices are the sole responsibility of the owner. MISD assumes no responsibility for personal computer devices, including, but not limited to a device being lost, loaned, damaged or stolen. Accordingly, limited MISD time or resources will be spent trying to locate stolen or lost personal computer devices. Each MISD Member is responsible for his/her personal device(s), including, but not limited to set up, maintenance, charging and security. MISD staff will not diagnose, repair or install software on a MISD Member's personal computer device. Should (1) prohibited, unacceptable and/or inappropriate use/access and/or (2) a security breach of the MISD Network that involves (or potentially involves) a MISD Member's personal computer device occur, be detected and/or suspected, appropriate MISD staff may search, examine, access, and/or inspect the MISD Member's personal device(s) in order to confirm or rule out any prohibited, unacceptable and/or inappropriate use/access and/or security breach involving the MISD Network.

c. Subject to System Administration: All MISD Network accounts and computer usage are subject to perusal by the MISD Network system administrator for virus scanning and monitoring for inappropriate use and investigation of suspected misuse at the authorized direction of MISD administration regardless of cause. No MISD computer/network/Internet usage (including usage by a personal computing device) shall be considered confidential. Accordingly, MISD Members should not use the MISD Network to send, receive or store any information, including any kind of electronic messages (email, text etc.), the MISD Member considers personal or confidential and wishes to keep private. All electronic files, including all electronic messages, transmitted through or stored in the MISD Network will be treated no differently than any other electronic file. MISD reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. MISD Members should treat the MISD Network like a shared or common file system with the expectation that all information and electronic files, sent, received or stored anywhere in the MISD Network system, will be available for review by any authorized representative of MISD for any purpose.

d. Required Training: All MISD Members will participate in annual training for appropriate technology use as well as copyright laws. In addition, MISD local and legal policy will require annual cybersecurity training. Employees who demonstrate vulnerabilities as a result of District digital drills will be required to attend additional training after each recorded incident.

IV. PROHIBITED, UNACCEPTABLE AND/OR INAPPROPRIATE USE: Prohibited, unacceptable and/or inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations by MISD, that violate the rules of network etiquette, or that interfere with, hamper or harm the integrity or security of the MISD Network, as well as the following:

a. Violation of Law: Transmission of any material in violation of any U.S. or State law is prohibited. This includes, but is not limited to: copyrighted material; threatening, harassing, or obscene material; or material protected by trade secret. Any attempt to break the law through the use of the MISD Network may result in litigation against the offender by the proper authorities. If such an event should occur, MISD will fully comply with the authorities to provide any information necessary for the litigation process.

b. Commercial Use: Use for commercial, income-generating or “for profit” activities, product advertisement, or political lobbying is prohibited.

c. Vandalism/Mischief: Vandalism and mischief are prohibited. Vandalism is defined as any malicious attempt to harm or destroy data or devices of another MISD Member, the MISD Network, or any other networks that are connected to the MISD Network. This includes, but is not limited to, the creation or propagation of computer viruses. Any interference with the work of other MISD Members, with or without malicious intent, is construed as mischief and is strictly prohibited.

d. Electronic Mail Violations: Forgery of electronic mail messages is prohibited. Reading, deleting, copying, or modifying the electronic mail of other MISD Members is prohibited. Sending unsolicited junk mail, spam, chain e-mails, or that of commercial content is prohibited. Using accounts (including the signature files) for non-school related activities including, but not limited to: financial gain, pornography/child pornography, personal advertising, buying, or selling, political activities (including lobbying), public relations and such activities as solicitation, fundraising, or religious activities is prohibited.

e. File/Data Violations: Deleting, examining, copying, or modifying files and/or data belonging to other MISD Members is prohibited.

f. System Interference/Alterations/Hacking: Attempts to exceed, evade or change resource quotas are prohibited. Installing unauthorized network access points or other connections, causing or attempting to cause network problems, including but not limited to, network congestion through mass consumption of system resources, attempts to disable the MISD Network filter or compromising the integrity of the firewall, and unauthorized access (hacking) into any part of the MISD Network are prohibited.

g. Inappropriate Speech/Messages: The following restrictions against inappropriate speech and messages apply to all communication sent and/or accessed through the MISD Network, including all emails, instant messages, texts, web pages, blogs, wikis, or other avenues of electronic communication. MISD Members shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages. MISD Members shall not post information that could cause damage, danger, or disruptions, or engage in personal attacks, including prejudicial or discriminatory attacks. MISD Members shall not harass another person or knowingly or recklessly post false or defamatory information about a person or organization. Personal political use to advocate for or against a candidate, office-holder, political party, or political position is prohibited. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit.

h. Home/Personal Internet: A MISD Member's home and personal electronic communication use (outside of the MISD Network) can have an impact on MISD and its schools, students and/or staff. A MISD Member's personal electronic communication expression including, but not limited to, threatening messages, a violent or sexual website, a text, or a post that creates a likelihood of material or substantial disruption of the school/district's operation may result in MISD disciplinary action and/or criminal penalties.

i. Bullying/Harassment: MISD takes cyber bullying and harassment by electronic communication very seriously, and it will not be tolerated. MISD Members shall not use the MISD Network to intimidate, threaten, bully, harass, or embarrass students or MISD Members. MISD Members who engage in such activity on school grounds or who engage in such activity off campus and create a material or substantial disruption of school operations (or the reasonable potential exists) shall be subject to disciplinary actions as well as possible criminal penalties.

j. Responding to communications that carry malicious attempts that are made over electronic mail or other digital mediums, including, but not limited to phishing, clicking on links containing malware or other data comproming programs, and opening documents containing malware or other data compromising programs.

V. CONSEQUENCES OF VIOLATION: Any attempt to violate the provisions of this Agreement will result in revocation of the MISD Member's account, regardless of the success or failure of the attempt. In addition, students may face MISD disciplinary action (Student Code of Conduct) and/or appropriate legal action. In the event of a claim that a student has violated these guidelines, MISD will provide the student with due process in accordance with the Student Code of Conduct. Staff members may face MISD disciplinary action up to and including employment termination and/or appropriate legal action.

a. Final Determination: The Superintendent or her/his designee will make the final determination as to what constitutes prohibited, unacceptable and/or inappropriate use.

B. Denial, Revocation, or Suspension of Accounts: The superintendent/designee, departmental director, campus principal, and/or the system administrator in accordance with MISD disciplinary procedures may deny, revoke, place restrictions, or suspend an account.

VI. SECURITY

a. High Priority: Security of the MISD Network is a high priority.

b. Reporting Security Problems: If a MISD Member identifies or has knowledge of a security problem on the MISD Network, the MISD Member must notify a teacher, campus principal, system administrator, and/or the superintendent's designee for MISD. The MISD Member shall not reveal or demonstrate the problem to others.

c. Impersonation: Attempts to login to the MISD Network as a system administrator or as another MISD Member may result in suspension of access to the MISD Network, as well as other appropriate disciplinary or legal action in accordance with the Student Code of Conduct or Board Policy.

d. Security Risks Denied Access: Any MISD Member identified as a security risk or having a history of problems with other computer systems may be denied access to the MISD Network.

e. Supervision: Staff must supervise student use of the MISD Network in a manner that is appropriate to the student's age and the circumstances of use.

f. Filtering Software: MISD Members may not disable the MISD Network filtering software at any time. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material if the filtering software has inappropriately blocked access to such sites.

g. Bandwidth: Bandwidth utilization is monitored. MISD Members who routinely monopolize excessive amounts of bandwidth will be notified and their usage will be examined. In order to protect and reserve bandwidth and other resources for educational use, MISD Members may not:

- Download software or files that are not for educational purposes;
- Play interactive online games
- View non-curriculum based streaming videos/movies; or
- Set their Internet web browser home page to a digital media rich site (i.e. CNN, Yahoo, MSN).

VII. INTERNET SAFETY: Internet safety of MISD Members in their use of the MISD Network is a high priority.

- DO NOT give your username/password to anyone.

- DO NOT tell anyone online your full name, home address, phone number, age, friend's name, your school, or any other personal information.

- DO NOT share photos of yourself, your family, or your home with people you meet online.

- DO NOT open attachments or click on the links in an e-mail from someone you do not know.

- DO NOT make appointments to meet people whom you meet online. Students should report to a teacher or administrator if they receive such a request. A MISD Member who becomes aware of prohibited, unacceptable and/or inappropriate use (defined above) should not respond; instead, a teacher or administrator should be notified immediately.

- DO NOT accept e-mails, files, or web page addresses (and the like) from strangers. People who you meet online are not always who they say they are. Be aware that online information is not necessarily private.

- DO report all suspicious emails to Technology Services using procedures outlined by the District

VIII. Equipment Issued

Equipment issued to employees is done so through the utilization of taxpayer funds. Physical care should be taken to ensure that the hardware is handled carefully and stored securely at all times. Staff members are required to report equipment that is malfunctioning immediately by securing a Technology Help ticket. Staff members are also required to file a police report and submit it on a Technology Help ticket if any hardware issued is stolen.

DISCLAIMER

MISD makes no warranties of any kind, whether expressed or implied, regarding or in connection with the MISD Network or any MISD Member's use or access thereto. MISD is not responsible for any damages claimed and/or suffered by any MISD Member from any use and/or access (or lack thereof) to the MISD Network. This includes loss, theft, or damage to personal devices; loss of data resulting from delays, non-deliveries, mis-deliveries; intrusion by computer virus; or other service interruptions or malfunctions. MISD is not responsible for phone/credit card bills or any other charges incurred by MISD Members. Use of any information obtained via the MISD Network is at the MISD Member's own risk.

MISD is not liable for any individual's prohibited, unacceptable and/or inappropriate use of the MISD Network including, but not limited to, electronic communication systems or violations of copyright restrictions or other laws or for costs incurred by MISD Members through use of the MISD Network. MISD shall not be responsible for ensuring the availability of the MISD Network or the accuracy, age appropriateness, or usability of any information found on the Internet.

Manor Independent School District

TECHNOLOGY DEVICE USE AGREEMENT

Please read this Agreement. Sign and return the last page.

General Information:

Manor ISD is distributing 1:1 technology devices to all grade students to use both in school and at home.

Devices will be assigned to the individual students based on their campus location and will be recorded in Manor ISD Technology Asset Inventory System.

This device is intended for student use only. The device has been configured to always remain connected to the Manor ISD network. Filtering measures have been installed in accordance with CIPA guidelines and are designed to only allow online access to the educational resources the student would typically use while on campus. While the district has installed filtering software on devices, we cannot guarantee blocking all inappropriate sites.

Devices are district property and must be returned when the student is no longer enrolled in Manor ISD.

Students who leave the district and fail to check in their device and any related equipment will have theft charges filed against them immediately upon the district's knowledge of such an event. The district will prosecute the occurrence to the fullest extent of the law**.**

The device is to be used in accordance with the District's Acceptable Use Agreement and Student Code Of Conduct

Internet access is not provided with the device. Students will need to connect to their own home wireless or use public wireless where available.

For technology devices to all 9th – 12th: Students will keep the device throughout their tenure in Manor ISD. It will not be necessary to return the device at the end of each academic year, unless the student is graduating or withdrawing from the district.

For technology devices to all Middle and Elementary: Students are not allowed to remove technology devices from campus unless instructed by the campus Principal. If a device is removed from campus, you will be charged the full amount for a replacement. Device coverage will only cover issues while on campus.

Student Responsibility:
Care of the device

- The device is the property of Manor ISD and should be kept clean and free of marks at all times. Writing or drawing on, engraving or otherwise defacing the device are not allowed and will result in loss of privileges, possible fine, and disciplinary consequences.
- Treat the device with care by not dropping it or gripping it by the screen.
- Do not leave your device in an unsecured area. This includes an unlocked locker or in public areas.
- Do not loan the device to anyone for any reason.
- Protect the device by unplugging the power supply and other peripherals when transporting it.
- Protect the display by carefully closing the lid when moving the device. Avoid objects left on the keyboard.
- Students should protect their device from extreme heat or cold. Devices should never be left in a car, even if the car is locked.
- Device should be protected from the weather, water or other liquid, food, and pets. Students should never eat or drink while using their device, or use their device near others who are eating or drinking.
- Heavy objects should never be placed or stacked on top of your device. This includes books, musical instruments, sports equipment, etc.
- Students should use care when plugging in any cords, cables, or peripheral into their device.
- Device should not be placed on or under soft items such as pillows, chairs or sofa cushions, or blankets. This could cause the device to overheat, and will result in damage to the device and possibly a fire.
- Clean the screen only with a soft, dry microfiber cloth. **Do not use Windex or other harsh chemicals to clean the screen**.

Student Device Coverage, Repair, and Replacement Information

Manor ISD is offering an opportunity for parents/guardians to purchase Technology Device Opt-In coverage which will cover ***accidental damage*** to the device issued to your student(s). Parents may opt-in for a $25 warranty coverage for the current school year, which will need to be paid for each student who has checked out a district device. **The coverage does not cover loss of the device, charger, OR damage due to user negligence**.

- If the device is damaged or not working properly, it must be turned in to the campus for repair or replacement.
- Parents/guardians and students are not authorized to attempt repairs themselves, or contract with any other individual or business for the repair of the device.
- **Theft or Damage must be immediately reported to the Help Desk at (512) 278-4999 or campus Principal**.
- A police report must be filed with the Manor ISD police department within 3 days of the device being stolen and a copy of the report must be made available in order to receive a replacement or loaner device. A fine for a replacement device can be required with no police report.

Please review the information below for details on the repair fees and coverage options. If you would like to purchase the opt-in coverage, click or copy the following link in a web browser and you will be redirected to

Technology Opt-In Coverage Payment Website

- Receipt of payment is generated automatically to the technology department for tracking.
- Technology Device Coverage is non-refundable.
- Coverage is renewable and can be purchased at the beginning of each school year.
- Devices assigned directly from Special Programs use such as CTE and SpEd are not part of the Technology Device Coverage Plan.

Repair Schedule Fees for Damage	**With Purchase of Device Coverage**	**Without Purchase of Device Coverage**
First Repair	No charge	No Charge
Second Repair	No Charge	$25.00
Third Repair	No Charge	$50.00
Device Replacement ***(due to unrepairable damage)***	**With Purchase of Device Coverage**	**Without Purchase of Device Coverage**
First replacement	No Charge	$275.00
Forth Repair (+) or Second and Subsequent Replacements	$275.00	$275.00
Device Replacement (Due to Loss or Stolen)	**With Purchase of Device Coverage**	**Without Purchase of Device Coverage**
Stolen Devices	Replaced at no Charge with Valid Police report	Replaced at no Charge with Valid Police report
Lost Devices	$275.00	$275.00
Lost Charger	$20.00	$20.00

Students may be loaned a device while their device is being repaired, provided the campus has some available. It will be at the campus' discretion on whether or not to loan a temporary device to a student if this is a second or subsequent repair.

If you have any questions regarding the Technology Device Coverage, please call the Help Desk at 512-278-4999.

- Receipt of payment is generated automatically to the technology department for tracking.
- Technology Device Coverage is non-refundable.
- Coverage is renewable and can be purchased at the beginning of each school year.
- Devices assigned directly from Special Programs use such as CTE and SpEd are not part of the Technology Device Coverage Plan.

Manor ISD Technology Device Use Agreement

We have read the device Use Agreement. We agree and understand the following: *(Please initial)*

______ We accept the responsibilities as stated in the agreement for the care and use of the device.

______ We accept the responsibilities regarding the repair or replacement of the device.

______ I **understand that if we leave the district and fail to check in the device and any related equipment, theft charges may be filed immediately upon the district's knowledge of such an event.**

_____ We have read and acknowledged that the district is offering an option for student device coverage.

Please initial one option you choose for device coverage

_____ I want to opt in for accidental coverage for my student and pay the $25 fee through Manor ISD RevTrack's website.

_____ I want to opt out of coverage for my student and assume all financial responsibility for lost, stolen, broken, damage or the repair costs for my student's issued device

Signed Device Use Agreement must be returned to the campus by October 1st or two weeks after enrollment date.