Marfa Independent School District
400 W Lincoln St
Marfa, TX 79843

Student Acceptable Use Policy for Technology Resources 2017-2018

<u>Please read this document carefully before signing.</u>

If the student is under the age of 18, a parent or legal guardian must also read and sign this agreement. Your signature on this document is legally binding and indicates the party who signed has read the (1) terms and conditions carefully, (2) understands the significance of this agreement, (3) and agrees to abide by all guidelines outlined in this agreement.

Student AUP

We are pleased to offer students of Marfa ISD access to the district computer network for educational purposes, including applications and the Internet. The following policy of usage has been adopted by Marfa ISD (also reference, Board Policy CQ(Local)).

Definition of District Technology Resources

The District's computer systems and networks are any configuration of hardware and software. The systems and networks include all technology hardware, software, infrastructure, data files, servers, workstations, sensors, tablets, internet devices, projectors, etc. This includes local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The District reserves the right to monitor all technology resource activity.

Internet/Technology Safety Policy - The Internet is a network connecting thousands of computers all over the world. With access to computers and people all over comes the availability of material that may not be considered to be of educational value in the context of the school setting.

• Marfa ISD has taken measures to block and/or filter access to undesirable and inappropriate sites to maintain compliance with the Child Internet Protection Act (CIPA). An undesirable and inappropriate site is hereinafter defined as “one that portrays or depicts violence, profanity, partial and/or full nudity, sexual acts or text, gross depictions or text, intolerance, cult, drugs and drug culture, militant or extremist, gambling, and/or alcohol related content”. While these protection measures are in place, it is impossible to filter all undesirable and inappropriate sites at all times. New sites are placed on the internet daily. As a result, students may inadvertently or purposely connect to an undesirable and inappropriate site. Should a student inadvertently access such a site, they should notify a staff member immediately. As soon as the district is aware of any such site, measures will be taken to filter the site. While it is the district's intent to make Internet access available to further educational goals and objectives, students may find ways to access other materials. Marfa ISD may monitor online activities of students without prior consent. Students caught visiting undesirable and inappropriate sites may be disciplined as outlined in section *Consequences of Improper Use – Students*. Marfa ISD firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the District.

• In accordance to the Protecting Children in the 21st Century Act, Marfa ISD will provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, to minimize the incidence of cyber predation/stalking whether in school or at home.

• "Cyber-bullying" is defined as bullying through the use of technology or any electronic communication by such things as email, internet communications, instant message, text message or facsimile. Cyber-bullying includes, but is not limited to:

○ ***Flaming***- deliberately sending/posting of electronic messages to a person(s) either privately or publicly.

○ ***Impersonation***- when a person pretends to be or poses as another person. Once the impersonator has access to the victim's information, considerable damage can occur.

○ ***Sending malicious code***- intentionally to damage/harm the victim's system or to spy on the victim.

○ ***Sending images and videos***- is a growing concern. Photographs and videos taken using cell phones of other students in bathrooms, locker rooms, or other compromising situations are easily distributed electronically, and sometimes published on video sites such as *YouTube*.

○ ***Trickery***- when a person purposely tricks another person into divulging secrets, private information or embarrassing information, and publicly discloses that information online.

○ ***Sexting***- sending, receiving, or forwarding sexually suggestive nude or nearly nude photos or sexually explicit or suggestive messages through text message or email, usually with the consent of all persons involved, however, once an image or message is digitized, it is very easy to forward to anyone, including unintended recipients.

It is the responsibility of every student, parent and employee of the school district to recognize acts of online predation, cyber-bullying and retaliation. Any student who believes that he or she has been the victim of such act should report it immediately to his or her teacher, principal or other school official so that measures can be taken to end the abuse. All forms of electronic harassment either during school hours or after school hours will not be tolerated by Marfa ISD.

Acceptable Use

Use of technology resources can be broadly categorized as acceptable, allowable, or prohibited:

§ Acceptable use of information technology resources is legal use consistent with the mission of the Marfa ISD, i.e., use that furthers the district's mission of learning and teaching.

§ Allowable use is legal use for other purposes that do not impinge on acceptable use. The amount of allowable use will vary over time based on the capacity reserve of information technology resources available beyond acceptable use.

§ Prohibited use is illegal use and all other use that is neither acceptable nor allowable.

Technology devices in education have grown to be an indispensable tool in the classroom, but to maintain their availability at a high level it is imperative that proper supervision always be exercised.

1. Devices use must be in support of education and research consistent with district policy.
2. Device use for commercial purposes is not acceptable.
3. Learn to properly credit any Internet sources just as you would conventional texts.
4. Do not waste school resources through improper use such as excessive printing or modifying a device's settings causing it to become unavailable to other users.
5. A limited amount of personal use of the device and Internet is acceptable. The definition of 'limited' is left up to the discretion of the Principal and Superintendent. Abuse may result in loss of access and other disciplinary action.
6. Storage devices (floppy, zip, CD-ROM or pen drives) provided by students wanting to bring in outside data or to take data from our computer system are not allowed unless approved of by an Administrator because of potential virus and malware problems.
7. No students or other children are permitted to work on technology devices unsupervised.
8. Unauthorized use of copyrighted software or material found on the Internet is prohibited without the written permission of the copyright holder.
9. No software may be loaded on any school device without the knowledge and permission of the technology office due to piracy and/or compatibility issues.
10. Participation in any chat room or news group is generally prohibited. For classroom use, some newsgroups may be permitted under a teacher's supervision.
11. Other Internet enabled devices are NOT PERMITTED during school hours, except with the permission and supervision of a teacher or administrator. This includes such items as iPods, PDAs, MP3 players, smart phones, and flash drives.
12. Access to any and all file-sharing sites is forbidden unless express permission for that particular site on that particular occasion is sought from your teacher and granted.
13. Access to any and all so-called "personal space" websites for online discussions (live or posted) and the posting of personal information (through blogs and such) is strictly forbidden.
14. DO NOT move any computer(s) or technology devices (AV Rovers, etc) without permission from the Principal, Superintendent, or Director of Technology.

Computer Etiquette

1. Use the technology systems **properly and sensibly**: use care with the devices.
2. **Be polite** to others whether they are physically beside you or using the device on the other end of your network connection.
3. Use caution when revealing any name, address or phone number. Students should not provide any information beyond their first name while communicating on the Internet.
4. Do not intentionally disrupt the network or another person's access to any computer device.

Inappropriate Language

1. Restrictions against inappropriate language apply to all speech communicated through the district's network system including public and private messages, material posted on Web pages, wikis, blogs, and any social networking sites.
2. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or symbols.
3. Do not post information that could cause damage or a danger of disruption to your school or any other organization or person.

4. Do not engage in personal attacks, including prejudicial or discriminatory attacks.
5. Do not harass or cyberbully another person. Cyber bullying includes but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, hate mail or terrorizing another student or staff member by way of any technological tool.
6. Do not knowingly or recklessly post false or offensive information about a person or organization.
7. Promptly disclose to your teacher or a staff member any message you receive from any other student that is in violation of the restrictions on inappropriate language.

Security

Each account is accessible through a username and password. These give the user certain access to computer devices throughout the system, the Internet, and possibly an email account.

1. Login to use a computer and remember to logout when you complete your task.
2. Internet access must be through the content filter. DO NOT attempt to by-pass the filter.
3. If you identify a security problem (virus, malware, etc.), notify a teacher or the Director of Technology immediately. Your data and account access may be at risk.
4. Do not reveal your account password or allow another person to use your account. If you suspect that another person is using your account, change your password immediately. Ask a teacher or administrator for assistance.
5. Attempts to log on as another user may result in loss of your access, loss of your account, loss of computer privileges or other disciplinary action to be determined by the principal.
6. Under certain conditions, your old account may be deleted and a new account created. Contact your teacher if you have a problem with your account.

Penalties

1. Any user violating these policies, applicable state and federal laws, or posted classroom and district rules is subject to loss of technology and network privileges and any other District disciplinary actions up to and including criminal prosecution.
2. School and District Administrators will make the final determination as to what constitutes unacceptable use. Their decision is final.

Damage

Marfa ISD will not be responsible for any damages a user may suffer, including the loss of data, damaged CDs, and the accuracy of information obtained through this Internet connection. Parents or guardians will be responsible for any damage, loss, and costs incurred by students based off the Marfa ISD Technology Pricing Sheet. This includes but is not limited to any technology items in a 1:1 environment or checked out by the library such as wifi hotspots, Chromebooks, iPads, power supplies, computers, internet devices, and tablets.

System Access

1. Prior to gaining access, system users are required to sign an agreement form that they have read and agree to abide by all district policy and regulations regarding district technology.
2. Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

Filtering

Marfa ISD will select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the School District. System users may not disable, bypass, or attempt to disable or bypass a filtering device on the District's electronic communications system.

Computer Software

Our goal is to promote the use of appropriate, innovative software whenever possible. These guidelines will insure that the required support and installation process is in place before funds are expended. Unauthorized software installation may affect network and machine performance adversely and is prohibited by the policy and administrative regulations of Marfa Independent School District Technology Resources. Under no circumstances will students install any kind of software on District computers. Only designated District personnel will install software.

Computer Hardware

1. Absolutely no one except approved vendors, district technicians, and designee are authorized to install computer hardware on any district site.
2. Hardware must be purchased through the current technology bid or with approval by the technology purchasing agent and meet the minimum hardware standards.
3. Campus computer systems may not be modified, upgraded, or replaced with donated equipment without the prior approval of the Technology Department.
4. In order to maintain an accurate inventory, computer systems may not be moved from one room to another except by the Technology Department and with the approval of the immediate supervisor. System users must submit a request via the technology work order system.

Monitoring of District Technology Resources

Monitoring can occur while engaging in routine maintenance, carrying out internal investigations, preparing responses to requests for public records, or disclosing messages, data, or files to law enforcement authorities. Monitoring can occur at any time to ensure appropriate use. The District reserves the right to monitor access to and use of the Internet or other network or computer-related activity.

The district respects the contents of your files and does not review or file content as a part of normal daily activities. However system administrators may become aware of file content while dealing with some system problems. Usage logs are frequently kept to diagnose such problems. Furthermore, the district will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance has included providing when required, copies of discussions on district operated mailing list servers, files, instant messaging, etc.

The district does not review electronic communication for the purpose of determining whether impermissible activity is occurring unless requested by campus or district administration. However in the course of assuring the viability of the district's network, system administrators may become aware of activity that poses a risk to the network's proper operation. In such cases staff may need to disable or block access to ports involved in traffic levels deemed to pose a risk to the network's optimal functioning. During the process of diagnosing potential problems to the network, any information obtained that indicates possible unauthorized distribution and/or procurement of copyrighted materials may be referred to an Administrator for further investigation.

Vandalism Prohibited

Any attempt to harm, deface or destroy District equipment, materials, data, or any of the agencies or other networks to which the District has access is prohibited. Intentional attempts to degrade or disrupt system performance may be viewed as violations of district policy and regulations and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33.

Vandalism as defined above will result in the cancellation of system use privileges and possible prosecution. The party will be responsible for restitution of costs associated with cleanup, system restoration, hardware, or software costs.

Suspension/Revocation of System Accounts

The District will suspend or revoke a user's access to the District's resources upon violation of District policy and/or administrative regulations regarding acceptable use. Termination of a student's access will be effective on the date the principal or campus coordinator receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Consequences of Improper Use

Improper, negligent, or unethical use may result in disciplinary actions consistent with the existing district policy, regulations, the Texas Penal Code, Computer Crimes, Chapter 33, or other applicable state and federal laws. This may also require restitution for costs associated with cleanup, system restoration, hardware, or software costs.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor-supplied hardware and software. Therefore, the District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the District’s.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's computer systems and networks.

What are the rules?

Privacy - Network storage areas may be treated like school lockers. Administrators may review communications to maintain system integrity to ensure that students are using the system responsibly.

Storage capacity - Users are expected to remain within allocated disk space and delete material which takes up excessive storage space.
Illegal copying - Students should never download or install any commercial software, shareware, or freeware onto network drives or disks. Nor should students copy other people's work or intrude into other people's files.
Inappropriate materials or language - No profane, abusive or impolite language should be used to communicate nor should materials be accessed which are not in line with the rules of school behavior. Should students encounter such material by accident, they should report it their teacher immediately.

YOU WILL BE HELD RESPONSIBLE AT ALL TIMES FOR THE PROPER USE OF YOUR ACCOUNT.

Important Guidelines to Follow

1. Do not use a computer to harm other people or their work.
2. Do not damage the computer or the network in any way.
3. Do not interfere with the operation of the network by installing illegal software.
4. Do not violate copyright laws.
5. Do not view, send, or display offensive messages or pictures.
6. Do not share your password with another person.
7. Do not waste limited resources such as disk space or printing capacity.
8. Do not trespass in another person's folders, work, or files.
9. Notify an adult immediately if you encounter materials that violate the rules in this AUP.
10. Be prepared to be held accountable for your actions and for the loss of privileges if the Rules of Appropriate Use that are stated in this AUP are violated.

Examples of Offenses

The following are examples of 1st, 2nd, and 3rd degree offenses. This list is not all inclusive.

1st Degree Offenses

- Using chat or other communication software.
- Changing system or network settings (i.e. screen saver, backgrounds).
- Access storage devices without prior permission from the instructor.

2nd Degree Offenses

- Using obscene language.
- Downloading, installing, or attempting to install software or files.
- Accessing or attempting to gain access to another user’s password or account.
- Giving a password or account to another user.
- Violating copyright laws (i.e. plagiarism).

3rd Degree Offenses

- Harassing, threatening, or attacking others through the use of the network (cyber-bullying).
- Damaging technology and/or computer networks including attempting to access systems to which the student has no authorization (i.e. hacking, spying, attempting to access proxies).
- Accessing or attempting to access, sending, or displaying offensive messages, pictures, or web sites (pornography or ‘hate’ sites).
- Employing the network for commercial use (i.e. selling video/music CDs, auction sites).

- Installing or attempting to install denial of service software (i.e. virus, sniffers).
- Stealing Marfa ISD property (i.e. hardware, software, peripherals, etc).
- Engaging in any activity which contravenes the laws of the United States.
- Connecting or attempting to connect personal computing devices to the MISD network (i.e. PSP, Personal Laptops with broadband cards, cell phones or any other personal data devices).

Consequences

The following are the repercussions for violating the Acceptable Usage Policy:

1st and 2nd Degree Offenses—Student, parent, teacher, and administrator conference will be required to assess and correct the problem. Student will be assigned to detention, in-school suspension or other disciplinary measures at the administrator's discretion. The student/parent will be held financially responsible for any necessary repairs, loss, damage, or vandalism occurring.

3rd Degree Offenses—Student computer access privileges will be revoked for the remainder of the school year, and the student/parent will be held financially responsible for any necessary repairs, loss, damage, or vandalism occurring. Loss of computer access privileges includes removal from all computer lab courses.

Habitual 1st or 2nd degree offenses can result in a 3rd Degree Offense consequence. Administrative action can include disciplinary or legal action including, but not limited to, criminal prosecution and/or penalty under appropriate state and federal laws.

The above rules are to assure every student is provided a computer on which to learn. The current rate of labor for repairs (subject to change) is $80.00 per hour (minimum of $30.00).

If you have any questions or concerns, please contact your child's campus administrator.

Consequences of Improper Use – Students - Improper or unethical use may result in disciplinary actions. Student actions not in compliance with the Student Acceptable Use Policy could result in:

❏ User account to technology services restricted in part, whole, or completely revoked
❏ Restitution for costs associated with system restoration, hardware, software, etc.
❏ Detention
❏ In-school Suspension
❏ Loss of class credit
❏ Permanent removal from class and/or assigned an alternative class
❏ Suspended or expelled from school
❏ Alternate education assignment
❏ Criminal charges filed
❏ The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's computer systems and network.