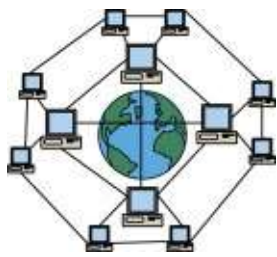# THE USE OF COMPUTERS AND THE INTERNET

PERMISSION FORM   2016-2017

Morgan Mill School is pleased to offer students access to a computer network for the Internet (all grades). To gain access to the Internet, all students must obtain parental permission as verified by the signatures on the attached form. Should a parent prefer that a student not have Internet access, use of the computers is still possible for more traditional purposes (word processing, spreadsheets, PowerPoint, educational software, etc.).

Please retain this letter and only return the permission form.

Internet access is designed to open doors and expand opportunities for all Morgan Mill ISD students. With increased technology and the use of Internet services, schools can teach students more about their global community. The use of the Internet is designed for educational purposes. Educators will monitor usage to determine if the Internet materials accessed are suitable for the educational arena. Violations may result in a loss of access as well as other disciplinary action. With the freedom to explore our educational resources comes **individual student** **responsibility**. Students are responsible for their behavior and communications over the network.

What is possible?

Access to the Internet will enable students to explore thousands of libraries, databases, museums, and other repositories of information and to exchange personal communication with other Internet users around the world. Families should be aware that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, or potentially offensive. While the purposes of the school are to use Internet resources for constructive educational goals, students may find ways to access other materials. We believe that the benefits to students from access to the Internet in the form of information resources and opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Therefore, we support and respect each family's right to decide whether to apply for access.

What is expected?

Students are responsible for appropriate behavior on the school's computer network just as they are in a classroom or on the school playground. Communications on the network are often public in nature. General school rules for behavior and communications apply. It is expected that users will comply with district standards and the specific rules set forth below. The use of the network is a privilege, not a right, and may be revoked if abused. The user is personally responsible for his/her actions in accessing and utilizing the school's computer resources. The students are advised never to access, keep, or send anything that they would not want their parents or teachers to see.

What are the rules?

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

Storage capacity -- Users are expected to remain within allocated disk space and delete e-mail or other material which take up excessive storage space.
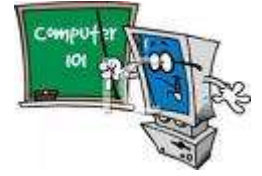
Illegal copying -- Students should never download or install any commercial software, shareware, or freeware onto network drives or disks, unless they have written permission from the Network Administrator. Students should not copy other people's work or intrude into other people's files.

Inappropriate materials or language -- Profane, abusive or impolite language should **_not_** be used to communicate nor should materials be accessed which are not in line with the rules of school behavior. A good rule to follow is never view, send, or access materials that you would not want your teachers and parents to see. *Should students encounter such material by accident, they should report it to their teacher immediately.*

These are guidelines to follow to prevent the loss of network privileges at school.

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, shareware, or freeware.
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's folders, work, or files.
9. Do notify an adult immediately, if by accident, you encounter materials that violate the guidelines of appropriate use.
10. BE PREPARED to be held accountable for your actions and for the loss of privileges if the Rules of Appropriate Use are violated.

Morgan Mill Independent School District (MMISD)
Internet Access Acceptable Use Policy

The purpose of the Morgan Mill Independent School District-provided Internet access is to facilitate communications and expand research/educational opportunities for faculty, administrators, and students. To remain eligible as users, use of the system must be in support of and consistent with the educational mission of MMISD. Access is a privilege, not a right. Access entails responsibility.

Any violation of the district's policy and rules relative to Internet or computer use may result in the loss of District-provided access. Additional disciplinary action may be determined at the campus or administrative level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may become involved.

Morgan Mill Independent School District-provided Internet users agree to the following:

Internet/network etiquette

- Be Polite
- Avoid use of vulgar or obscene language
- Use caution when giving out addresses or phone numbers (both yours and others)
- Remember, electronic mail is not private or secure
- Do not intentionally disrupt the network or other network users
- Abide by generally accepted rules of network etiquette

Usage guidelines and policies:

- Commercial use or political lobbying using these electronic resources is prohibited.
- Copyrights and others' intellectual property rights are to be observed at all times. Copying of files, software, or passwords belonging to others may constitute theft, plagiarism, or fraud. Software licensed to MMISD must be used in accordance with terms of the software license.
- Users must always identify himself or/herself in electronic communications. Anonymous or pseudo-anonymous communications appear to dissociate individuals from responsibility for actions. Concealing user identities or misrepresenting user's names or affiliations to mask or attempt to distance himself or/herself from irresponsible behavior is a serious abuse of the system. It violates local policies and constitutes fraud.
- Follow all security restrictions. Security on any computer system is a high priority, especially when the system involves many users. Do not reveal account passwords or allow others to use any account. Trying to evade, disable, or "crack" a password or other security provision is grounds for immediate suspension of access privileges and other disciplinary action. Users will be held responsible for any misuse of passwords. A user who is identified as a security risk or having a history of problems with other computer systems may be denied access to all MMISD Internet services.
- Respect the rights of others to freedom from harassment or intimidation. Harassment targets another person or organization to cause distress embarrassment, injury or unwanted attention, or other substantial discomfort. This includes, but is not limited to, the sending of unwanted email or chat line comments.

- Use resources efficiently. Please respect the fact that unlimited resources are not available. Time, network bandwidth, printers, paper, disk space, and terminals or PCs are all limited. Restrictions may be placed on any or all of these, as well as any other computing resource. Such restrictions are designed to ensure access for all users.
- There is no guarantee of privacy. Electronic communications should not be considered private or secure. In the course of diagnosing or correcting problems, system administrators may view the contents of any communications.
  Obscene communication of any kind, including text of graphic material, is prohibited. This includes any sexually explicit image or other content as specified by local, state, federal, or international laws or policies.
- Abide by the policies or guidelines of the network being used. Users are subject to all the rules, regulations or policies of other networks or computer services contacted or connected to from the school or home.
- Vandalism is prohibited. Vandalism is defined as any malicious attempt to harm or destroy data and/or equipment of MMISD, another user, the Internet, or other networks. This includes, but is not limited to, creating and/or uploading computer viruses.
- MMISD will not be responsible for any damage that users may suffer. This includes loss of data resulting from delays, non-deliveries or service interruptions caused by network failures, computer viruses, or users' errors or omissions. Use of any information obtained via network services is at the users' own risk. MMISD denies any responsibility for the accuracy or quality of information obtained through network services.

Penalties

MMISD regards any violation of this policy as a serious offense. Any student, staff, or board member violating these provisions, applicable state or federal laws, or policies of any of the local network are subject to loss of Internet/Network privileges and any other disciplinary options available, including criminal prosecution.

- Student cases shall be handled by the administration. Staff and faculty cases shall be handled by a committee appointed by the Superintendent.
- These bodies shall make the final determination of what is acceptable use. MMISD Board Policy DGBA (Local), FNG (Legal), and FNG (Local) outline procedures to process appeals or file grievances.

Harassment Complaints

Rules and regulations as outlined in MMISD Board Policy DAA, DHB, DHC, FB, FNCJ, FNCL shall be enforced in processing harassment complaints filed by users.

Morgan Mill ISD Internet Safety Policy
CIPA Compliant

Introduction

It is the policy of Morgan Mill School District ("The School District") to : (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA"). It is the goal of this policy not only to prevent and protect, but to educate employees, students, parents, and the community of MMISD in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by the School District into its Acceptable Use Agreement.

The Children's Internet Protection Act, enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities.

This policy is intended to be read together with the School District's Acceptable Use Policies for Technology and the Internet. All limitations and penalties set forth in the Acceptable Use Policies are deemed to be incorporated into this policy. Terms used in this policy which also appear in the Children's Internet Protection Act have the meanings defined in the Children's Internet Protection Act.

Compliance with the requirements of CIPA:

Technology Protection Measures

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. AISD utilizes a sophisticated content filtering system, on all computers that access the Internet, which is compliant with CIPA and NCIPA.

Access to Inappropriate Material

To the extent practical, Technology Protection Measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to administrative approval, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Any attempt to bypass, defeat or circumvent the Technology Prevention Measures is punishable as a violation of this policy and of the Acceptable Use Policies.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the MMISD online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the Acceptable Use Policy.

Specifically, as required by the Children's Internet Protection Act, prevention of
Inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all professional employees (pedagogical and administrative staff) of MMISD to supervise and monitor usage of the School District's computers, computer network, and access to the Internet in accordance with this policy, the Acceptable Use Policy, and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the chief technology officer or designated representatives.

Education

MMISD will advocate and educate employees, students, parents and the MMISD community on Internet safety and "cyber-bullying." Education will be provided through such means as professional development training and materials to employees, PTF presentations, CyberSmart week, and the School District website.

Cyber-bullying

The Acceptable Use Policies include provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying.

The School District is a place of tolerance and good manners. Students may not use the network or any School District computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

Network users may not use vulgar, derogatory, or obscene language.

Network users may not post inappropriate anonymous messages or forge e-mail or other messages.

Furthermore, School District computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, State of Texas or local laws. This includes, but is not limited to any threat or act of intimidation or harassment against another person.

Adoption

This Internet Safety Policy was adopted by the Board of Morgan Mill ISD at a public meeting following normal public notice on June 11, 2012.

User Agreement and Parent Permission Form
2016 - 2017

As a user of Morgan Mill School and Education Service Center Region XI Consortium, I agree to comply with the stated rules and instructions of all teachers when using the computers and Internet.

Student Signature_____

A parent may sign for the younger students.

Grade_____

As the parent or legal guardian of the minor student signing above, I grant permission for my child to have the following selected privileges. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for the guidance of Internet use and the conveying of standards to my daughter or son to follow when selecting, sharing, or exploring information and media.

Parent Signature _____

Date_____

Home Telephone_____ **Cell Phone** _____

E-mail address _____(optional)

_____ My child **may** use the Internet while at school according to the rules outlined.

_____I would prefer that my child **not** use the Internet while at school.

Please sign and return.