May ISD

Student/Parent Technology Handbook
And
Acceptable Use Policy
2015-2016

Board Approved January 2015

Student/Parent Device Handbook
Table of Contents

Computer Specifications

You can find out more information about District issued devices and updates for this student handbook at: www.mayisd.com.

Terms of the Device Loan

Terms: Students will make arrangements to pay an annual nonrefundable maintenance fee of $25 before taking possession of the device. Students will comply at all times with the May ISD Parent/Student Technology Handbook and Acceptable Use Policy, incorporated herein by reference and made a part hereof for all purposes. Any failure to comply may terminate your rights of possession effective immediately and the District may repossess the device.

Title: Legal title to the device is in the District and shall at all times remain in the District. Your right of possession and use is limited to and conditioned upon your full and complete compliance with this Agreement and the Parent/Student Device Handbook.

Loss or Damage: If the device is damaged, lost or stolen, you are responsible for the reasonable cost of repair or its fair market value on the date of loss. Loss or theft of the device must be reported to the District by the next school day after the occurrence. Seniors must clear all records and pay all fees before participating in graduation ceremonies.

Repossession: If you do not timely and fully comply with all terms of this Agreement and the Parent/Student Device Handbook, including the timely return of the device, the District shall be entitled to declare you in default and come to your place of residence, or other location of the device, to take possession of the device.

Term of Agreement: Your right to use and possession of the device terminates no later than the last day of the school year unless earlier terminated by the District or upon withdrawal from the District.

Appropriation: Your failure to timely return the device and the continued use of it for non-school purposes without the District's consent may be considered unlawful appropriation of the District's device.

Maintenance Fee

Students will pay an annual non-refundable maintenance fee of $25 to cover the costs associated with non-warranted items at the beginning of each school year to checkout a district device.

• Students will make arrangements to pay the fee before taking possession of the device.

• In case of theft, vandalism, and other criminal acts, a police report MUST be filed by the student or parent within 24 hours of the occurrence. Incidents happening off campus must be reported to the police by the parent and a copy of the report be provided to the school. Upon completion of the investigation the District may assess a replacement fee for the device.

• If device is lost, students/parents are responsible to pay for the fair market value to replace the device (see Fair Market Value chart).

• Student will be charged the full price of the device if deliberately damaged or vandalized.

• Seniors must clear all records and pay all fees before participating in graduation.

• Students/Parents are responsible for reasonable cost of repair for damaged devices.

Device Table of Fair Market Value

Age of Device	Laptop's Value	Tablet's Value
1 year or less	$750	$650

2 years	$600	$550
3 years	$450	$450
4 years	$300	$350

The costs of any other parts needed for repairs will be based on manufacturer's current price list. **Deliberate damage will be priced according to the actual cost of repair.**

Financial Hardships

Based on TEC 11.158, the school District may require payment of a reasonable fee, not to exceed the actual annual maintenance cost for the use of musical instrument, [technology] and uniforms owned or rented by the District.

If this fee creates a financial hardship on the student or parent from obtaining a device, please contact the campus administration about options regarding payment of the fee.

The administration will:

• Provide payment options for the student to pay out the fee over time

• Allow the student to provide hardship qualification information to campus Administration

(Reference Device Payment Option Form – Provided in Student Packet)

Use of Computers and Devices on the Network

May ISD is committed to the importance of a student being able to continue with his/her work when his/her device is experiencing problems. To assist with this problem the District is providing the following:

Network Student Drives

The students will have a network drive setup from their login. Students can save important items on this network drive, keeping a backup that they can access from anywhere on the network.

Loaning or Borrowing Devices

· Do NOT loan devices or other equipment to other students.

· Do NOT borrow a device from another student.

· Do NOT share passwords or usernames with others.

Classroom Assignments and Websites

Many classes will have online assignments posted on the District website which can be accessed through any computer with Internet access. Talk with your student's teachers about the availability of coursework and assignments on District website.

Internet Safety

There are many sites on the Internet that can be potentially dangerous to minors. These sites are blocked while students are logged on to the District network, but may be unprotected at home. Students are in violation of District policy if they access these sites through proxies. Parents may want to restrict their home access.

Additional Sources of Internet Safety Information:

FBI Parent's Guide to Online Safety:
 http://www.fbi.gov/publications/pguide/pguidee.htm

Internet Safety: http://www.isafe.org

NetSmartz: http://www.netsmartz.org/netparents.htm

Screensavers

• Inappropriate media may not be used as a screensaver.

• Presence of weapons, pornographic materials, inappropriate language, alcohol, drugs, gang related symbols or pictures will result in disciplinary actions.

• Passwords on screensavers and power-on screen are **not** permitted.

Sound

• Sound will be muted at all times unless permission is obtained from the teacher for instructional purposes.

• No headphones except for instructional purposes.

Deleting Files

• Do not delete any system folders or files that you did not create or that you do not recognize. Deletion of certain files will result in computer failure and will interfere with your ability to complete class work and may affect your grades.

• There is a $50 reimaging charge. Reimaging the device will result in the loss of ALL personal data.

Music, Games, or Programs
• Any music downloaded or streamed over the Internet must be appropriate as per District policy.

• Any games streamed over the Internet must be appropriate as per District policy.

• Decisions regarding appropriate music and games will be at the discretion of the Campus Administration.

• All software on the system must be District approved and installed by the Technology Department.

• All copyright laws will be enforced.

• There is a $50 reimaging charge to remove any of the above items. Reimaging the device will result in the loss of ALL personal data.

Unauthorized Access

Reference Board Policy CQ Local at
http://pol.tasb.org/Policy/Download/236?filename=CQ(LOCAL).pdf

Transporting Devices

• Devices must be transported in school provided cases and must remain in cases at all times.

• To prevent system damage, devices need to be closed and placed in school provided cases.

• Devices do NOT have to be shut down (turned off) between classes.

• Devices can be left on around the clock. Batteries must be fully charged prior to arriving at school each day.

Student Acceptable Use Policy for Technology Resources

These guidelines are provided so students and parents are aware of the responsibilities students accept when they use District-owned computer hardware, devices, operating system software, application software, stored text, data files, electronic mail, local databases, CDROMs, digitized information, communications technologies and internet access. In general, this requires efficient, ethical and legal utilization of all technology resources.

According to Texas Education Code Section 37.007 (b), a student may be **expelled** if the student:

(5) engages in conduct that contains the elements of the offense of breach of computer security under Section 33.02, Penal Code, if:
    (A) the conduct involves accessing a computer, computer network, or computer system owned by or operated on behalf of a school district; and
    (B) the student knowingly:

(i) alters, damages, or deletes school district property or information; or
(ii) commits a breach of any other computer, computer network, or computer system.

1. Expectations

a. During the class period, student use of computers, other technology hardware, software, and computer networks, including the Internet is only allowed when supervised or an instructional staff member has granted permission.

b. All users are expected to follow existing copyright laws.

c. Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

2. Unacceptable conduct includes, but is not limited to the following:

a. Using the network for illegal activities, including copyright, license or contract violations, downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.

b. Using the network for financial or commercial gain, advertising, or political lobbying.

c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as, but not limited to, pornographic sites.

d. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.

e. Causing congestion on the network or interfering with the work of others, e.g., streaming games, movies, or broadcasting messages to lists or individuals.

f. Degrading bandwidth and overusing finite resources which include constant streaming of any media while at school, i.e., online time, real-time music.

g. Gaining unauthorized access anywhere on the network.

h. Revealing the home address or phone number of one's self or another person.

i. Invading the privacy of other individuals.

j. Using another user's account, password, or ID or allowing another user to access your account, password, or ID.

k. Coaching, helping, observing or joining any unauthorized activity on the network.

l. Forwarding/distributing E-mail messages without permission from the author.

m. Posting anonymous messages or unlawful information on the system.

n. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous.

o. Falsifying permission, authorization or identification documents.

p. Obtain copies of, or modify files, data or passwords belonging to other users on the network.

q. Knowingly placing a computer virus on a computer or network.

3. Acceptable Use Policy – May Independent School District

a. General Guidelines

Students will have access to all available forms of electronic media and communication which is in support of education and research and in support of the educational goals and objectives of the May Independent School District.

Students are responsible for their ethical and educational use of the computer online services at the May Independent School District.

All policies and restrictions of the computer online services must be followed.

Access to the May Independent School District computer online services is a privilege and not a right. Each employee, student and/or parent will be required to sign the Acceptable Use Policy Agreement form and adhere to the policy at all times.

The use of any computer online services at the May Independent School District must be in support of education and research and in support of the educational goals and objectives of the May Independent School District.

When placing, removing, or restricting access to specific databases or other computer online services, school officials shall apply the same criteria of educational suitability used for other education resources.

Transmission of any material which is in violation of any federal or state law is prohibited. This includes, but is not limited to: confidential information, copyrighted material threatening or obscene material, and computer viruses.

Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the May ISD Student Code of Conduct.

Any parent wishing to restrict their children's access to any computer online services will provide this restriction request in writing. Parents will assume responsibility for imposing restrictions only on their own children.

b. Network Etiquette
- Be polite.
- Use appropriate language.
- Do not reveal data (home address, phone number, or phone numbers of other people).

Remember that the other users of the computer online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

c. Copyright

All applicable laws and statutes that protect the creative rights of intellectual material as defined in the copyright laws will be respected at all times by all students of the District and all persons employed by the District.

Copyrighted materials, including computer software, video films, and computer generated art, will not be utilized on any equipment owned by the District unless a license has been obtained granting such rights to the District.

Copyrighted materials legally licensed by the District for use by its students and/or employees will not be copied or removed from the District for use on equipment owned by individuals unless the license obtained by the District specifically grants rights for such use.

Copyrighted materials for which individual students or employees have obtained a license may not be installed or utilized on equipment owned by the District.

The District will establish and maintain a central inventory database where all license for use of copyrighted materials will be recorded.

If any student or employee of the District acquires the legal license to use copyrighted materials for the District, it is the responsibility of the person acquiring the materials to notify the Technology Director of such acquisition, the date of the acquisition, the source from which the materials were acquired, and the number of copies legally permitted by such license. If the acquiring individual does not properly notify the Technology Director, all copies of the software will be deleted from all District equipment.

Additional References – May ISD Handbook

d. E-Mail

- E-mail should be used for educational or administrative purposes only.
- E-mail transmissions, stored data, transmitted data, or any other use of the computer online services by students, employees or other users shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.
- All e-mail and all contents of the device are property of the District.

- Unauthorized use of another individuals USER ID to send, receive, or read electronic mail is improper.
- Use of District e-mail facilities should NOT be extended to Non-District employees
  or Non-District students.
- Unauthorized alteration or deletion of e-mail is inappropriate.

District e-mail facilities may NOT be used for any of the following purposes:

1. Sending chain letters;

2. Sending copies of documents in violation of copyright laws;

3. Forwarding e-mail messages without a legitimate District business purpose and/or forwarding messages under circumstances likely to lead to the embarrassment of the sender or to violate the clearly expressed desire of the sender to restrict additional dissemination;

4. Sending messages that have restricted access due to federal, state, or District\ regulations; or

5. Sending messages or soliciting messages that are obscene, that harass, or that are sent to promote a religious, political, or other personal position not associated with duties as an employee of District.

If a student, employee, or the administration is unwilling to see the message on the evening news or in the newspapers, it should not be sent.

e. Website and Media Publishing Standards

The following Standards will apply to all web sites developed and published in the name of May Independent School District on the World Wide Web or a District Intranet:

Any web pages that are created and maintained in the name of any part of May Independent School District must follow all policy regulations of the school board and District even if the web pages are maintained on a server not owned and operated by May ISD.

Web pages for educational purposes will be housed on the District web server. All

District policies and regulations including those regarding the Internet must be followed.

To access the District web server, an account will be established in the name of a school District employee. Only this employee will have access privileges.

The Technology Department will authorize the creation of any website and verify the website meets all District policies and regulations.

The campus or department is responsible for maintenance and upkeep of their portion of the website.

Any links connected to a District approved website must meet District policy and regulations.

All copyright laws must be followed. One should assume that use of anything found on the Internet or the World Wide Web is restricted unless the author gives notice that it is not.

Students or employees must obtain a release form to electronically display original work.
A release form must be obtained from a parent or guardian before allowing a photograph of a student or any other personally identifiable information to be posted on an Internet page under the District's control.
The District will not host or endorse any student's personal website. If a student creates a website for educational purposes, District guidelines apply. (See Student Media Release Policy for details)

The District may restrict the size of a website because of server space.

If the user does NOT want to claim copyright for a work published on the Web, the user must include a statement that allows copying and specifies the conditions for such permission.

Student Code of Conduct – Misbehaviors & Consequences

Phase I Misbehaviors	Phase I Consequences

Phase I misbehaviors include any student action deemed by instructors and/or administrators to Negatively affect the educational efficiency of the program.
 	
In addition to the infractions from Board Policy – Phase I Misbehavior will also include:
    Downloading screensavers, games, and/or music that is not instructional.
    Deleting instructional applications.
    Loss or vandalism of power cords
    Sharing identification or password with another person.
    Using another person's password.
    Trespassing, deleting, examining, copying, or Modifying files, data, or work belonging to others without prior consent.
    Intentionally wasting limited resources, including the distribution of "chain letters."
    Employing the network for commercial purposes, political activities, or private business.
    Revealing the personal address, Social Security number, account number(s), or phone number of yourself or any other person.
    Plagiarizing material or information from any electronic technological resources.
	Consequences of Phase I misbehaviors include, but not limited to, the following:
	
	First Offense:
	    Documentation in the Event Log found in Technician Workroom.
	    $50 re-imaging charge to correct misuse.
	    Cost to replace lost part
	
	Second Offense:
	    Written Warning
	    Call to parents
	    $50 re-imaging charge to correct misuse.
	    Cost to replace lost part
	
	Third Offense:
	    Removal of device pending Parent Conference
	    Parent Conference
	    $50 re-imaging charge to correct misuse.
	    Cost to replace lost part

MISBEHAVIOR: LEAVING DEVICES UNATTENDED OR USING DEVICES IN A MANNER THAT MAY CAUSE DAMAGE OR IS IN DIRECT VIOLATION OF DISTRICT POLICY	**CONSEQUENCE:** DEVICE WILL BE CONFISCATED AND HELD BY ADMINISTRATION PENDING A PARENT CONFERENCE.
Phase II Misbehaviors Phase II misbehaviors are more severe and persistent, this may be the fourth or more offenses of Phase I misbehaviors. In Phase II, student's conduct infringes upon the rights of others has negatively impacted learning. Damages and vandalism to hardware are included in Phase II misbehaviors: In addition to the infractions from Board Policy –	Phase II Consequences **Student is responsible for expenses incurred for intentional hardware damage.** Consequences of Phase II misbehaviors are at the discretion of the campus administrator and include, but are not limited to, the following: 1. Removal of device pending Parent Conference 2. Mandatory Parent Conference

Phase II Misbehavior will also include:

   Keyboard, hard drive, screen…damaged and Requires replacement.

   Student distributes illegally obtained electronic materials.

   A violation of policy that negatively impacts the rights of another student.

   Creating, accessing, or processing offensive or pornographic messages or pictures; obscene or threatening language; and harassing, hate related or discriminatory remarks.

   Damaging or injecting viruses into computers, computer systems, or computer networks.

   Employing the network for commercial purposes, political activities, or private business.

   Revealing the personal address, Social Security number, account number(s), or phone number of yourself or any other person.

   Transmission of any material in violation of any U.S. or state regulation.

   Violating copyright laws, including installation of Copyrighted software.

3. Behavior contract.
4. In---School Suspension
5. Suspension (based on repeated Phase II and behavioral offenses)
6. Notification of outside agency and/or police with filing of charges where appropriate.

If misbehavior results in legal action – assignment to an alternative education program will be a possible consequence.

Phase III Misbehaviors

Phase III misbehaviors are such that the student has disrupted or threatens to disrupt the school's efficiency to such a degree that his/her presence is not acceptable. Common signs of Phase III misbehaviors include, but are not limited to, the following offenses committed on school property or within 300 feet of school property, or while attending a school sponsored or school related activity except as noted. In addition to the infractions from Board Policy – Phase II Misbehavior will also include:

   Electronic threats

   Habitual violation of Level I & Level II offenses.

   Transmission of any material in violation of any U.S. or state regulation.

   Engaging in conduct that contains the element of breaching computer security under Section 33.02(b)(1) of the Texas Penal Code.

   Use or possession of hacking software or any other software capable of causing harm.

Phase II Consequences
Student is responsible for expenses incurred for intentional hardware damage.
Consequences of Phase II misbehaviors are at the discretion of the campus administrator and include, but are not limited to, the following:
1. Removal of device pending Parent Conference
2. Mandatory Parent Conference
3. Behavior contract.
4. In---School Suspension
5. Suspension (based on repeated Phase II and behavioral offenses)
6. Assignment to an alternative education program and notification of placement sent to the juvenile justice system.
7. Notification of outside agency and/or police with filing of charges where appropriate.
8. Permanent loss of device privileges.

Sec. 33.02. BREACH OF COMPUTER SECURITY. (a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner. (b) *[amended 9/1/97]* An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:

Student Pledge for Device Use

1. I will take good care of my device and know that I will be issued the same device each year---as long as I attend May ISD.
2. I will never leave the device unattended.
3. I will never loan out my device to other individuals.
4. I will know where my device is at all times.
5. I will charge my device's battery daily.
6. I will keep food and beverages away from my device since they may cause damage to the computer.
7. I will not disassemble any part of my device or attempt any repairs.
8. I will protect my device by only carrying it while in the case provided.
9. I will use my device computer in ways that are appropriate and educational.
10. I will not place decorations (such as stickers, markers, etc.) on the District device, power cords or carrying case. I will not write on the device, power adaptor, or carrying case. I will not remove any District applied labeling from the device, power adaptor, or carrying case.
11. I understand that my device and carrying case are subject to inspection at any time without notice.
12. I will follow the policies outlined in the Technology Handbook and the Acceptable Use Policy

while at school, as well as outside the school day.

13. I will file a police report in case of theft, vandalism, and other acts covered by insurance.
14. I will be responsible for all damage or loss caused by neglect or abuse.
15. I agree to pay for the replacement of my power cords, battery, or device case in the event any of these items are lost, stolen, or damaged.
16. I agree to return the District device and power cords in good working condition.

Student Name (Please Print):_____

Student Signature: _____ Date:_____

Parent Signature: _____ Date:_____

May Independent School District

STUDENT/PARENT TECHNOLOGY USE AGREEMENT

2015-2016

PLEASE PRINT ALL INFORMATION

Student Name: _____ _____
                          Last Name   First Name

Parent Name:_____ _____
                          Last Name   First Name

Parent Email Address: _____

Address_____

Home Phone: _____   Work/Mobile Phone: _____

Driver's License #: _____

Parent Date of Birth: _____

User's Signatures:

_____	_____	_____
Parent or Guardian Signature	Student Signature	Date

To be filled out by school district personnel upon student's receipt of device.

Item Description	Serial #	Condition
Device		
Charger		
Device Case		

In this agreement, "we", "us", and "our" means May ISD. "You" and "your" means the parent/guardian and student enrolled in May ISD. The "property" is a device owned by May ISD.

Term: You will comply at all time with the May ISD's Parent/Student Device Handbook and

Acceptable Use Policy, incorporated herein by reference and made a part hereof for all purposes. Any failure to comply may terminate your rights of possession effectively immediately and the District may repossess the property.

Title: Legal title to the property is in the District and shall at all times remain in the District. Your right

of possession and use is limited to and conditioned upon your full and complete compliance with this Agreement and the Parent/Student Device Handbook.

Loss or Damage: If the property is damaged, lost or stolen, you are responsible for the reasonable cost of repair or

its fair market value on the date of loss. Loss or theft of the property must be reported to the District by the next school day after the occurrence.

Repossession: If you do not timely and fully comply with all terms of this Agreement and the Parent/Student

Device Handbook, including the timely return of the property, the District shall be entitled to declare you in default and come to your place of residence, or other location of the property, to take possession of the property.

Terms of Agreement: Your right to use and possession of the property terminates not later than the last day of the

school year unless earlier terminated by the District or upon withdrawal from the District.

Appropriation: Your failure to timely return the property and the continued use of it for non---school purposes

without the District's consent may be considered unlawful appropriation of the District's property.

Internet Safety Tips for

Parents

LOCATION: The Device should be in a central location in the home where you can see it and monitor use.

You should be able to see their computer screen while they are online.

If they take the Device to other friends' homes, talk with their parents about how they monitor online access.

Spend time with your children online. Have them teach you about their favorite online destinations.

MONITOR: Monitor your child's computer use. Limit Internet, email, instant messaging, and chat room access.

Make sure you know where your child is going online, where he/she's been, and with whom.

Closely monitor your child's participation in any chat room.

Make sure you understand how your children are using the computer, what web sites they are visiting, and who they are communicating with online.

Always maintain access to your child's online account and randomly check his/her email. Be upfront with them about your access and the reasons why.

COMMUNICATE with your child about your expectations and what you consider appropriate for him/her while they are online.

Online tips to discuss with your student:

1. Never give out any type of personal information to anyone on the Internet. (Including name, address, phone, age, family income, friend's names, school location, photos, etc.)

2. Never use your parent's credit card on the Internet without their permission and supervision. Credit cards should never be used on sites that are not secure.

3. Never share passwords with anyone. When selecting passwords to use on the Internet, do not pick something that could easily be figured out or deciphered or is a common term.

4. Never arrange a face-to-face meeting with anyone you have met on the Internet. People you meet in a chat room may not be who they appear to be; Sally who says she's 12 can really be Bob who is 45.

5. Never open emails if you do not know whom they are from or if they make you feel uncomfortable in any way. Unsolicited e-mail that is opened could give you a virus and be the cause of unwanted mail (spam).

6. Never click on banner ads in a site. Most of the time, they will add your address to a database and you will receive unwanted spam mail.

7. Never use bad language or send mean or threatening email. Never joke around about inappropriate things when emailing others. Likewise, never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing.

8. Never upload (post) pictures of yourself or your friends/family to the Internet or online service to people you do not personally know.

Additional Sources of Internet Safety Information:

NetSmartz:

http://www.netsmartz.org/netparents.htm

FBI Parent's Guide to Online Safety:

http://www.fbi.gov/publications/pguide/pguidee.htm