

# Albany ISD Student Laptop Policy

## Table of Contents

### Terms of the Laptop Loan

### Use & Maintenance Fee

### Laptop Security

If a laptop needs to be reimaged for any reason all personal data will be lost. The student needs to take one of the following precautions to prevent loss of documents.

### iTunes Information

### Music, Games, or Programs

### Screensavers

### Fair Market Value

### Table of Fees, Fines, & Repair Costs

### Table of Estimated Repair Pricing

### Financial Hardships

### Use of Computers and Laptops on the Network

### Student Acceptable Use Policy for Technology Resources.

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

### Acceptable Use Policy - Albany Independent School District

Network Use and Content:

Inappropriate Use:

### Technology Offenses and Disciplinary Actions

Level I Technology Offense

### Texas Penal Code

### Internet Safety Tips for Parents

### Student Expectations for MacBook Use

### Keyboard Shortcuts

## **Terms of the Laptop Loan**

### **Terms:**

You will pay a nonrefundable annual use and maintenance fee of \$25 on or before taking possession of the property. You will comply at all times with the Albany School District's Parent/Student Laptop 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 property.

### **Title:**

Legal title to the property is to the District and shall at all times remain to 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 Laptop 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. A table of estimated pricing for a variety of repairs is included in the Parent/Student Laptop handbook to which reference is hereby made. 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 Laptop 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.

### **Term 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 return the property in a timely manner 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.

## Use & Maintenance Fee

- Students will pay a non-refundable annual use & maintenance fee of \$25\*.
- Students will pay fee on or before taking possession of the laptop.
- The student or parent **MUST** file in case of theft, vandalism, and other criminal acts, a police report **within 48 hours of the occurrence. Incidents happening off campus must be reported to the police by the parent and a copy of the report is brought to the school.**
- If laptop is stolen and student reports the theft (by the next school day) and police filed a report, then the student will not be charged the full price of replacement, just the \$200 insurance deductible.
- **Student will be charged the Fair Market Value of the laptop if lost, 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 deliberately damaged laptops (see Repair Pricing chart).

## Laptop Security

Each of the laptops has a security program installed on it. We have tried to strike a balance between usability of the equipment, and appropriate security to prevent the units from being damaged or used to cause damage to the Albany ISD system. Two forms of security exist:

1. Desktop Security - Security is in place on the desktop to prevent certain activities. These include downloading or installing software in the laptops, removing software, changing system settings, etc.
2. Filtering Software - Albany ISD maintains an Internet filtering software package on-site. This program automatically filters all student access to the Internet.
  - a. Reporting – Custom reports are generated by username, ip and machine name.
    - i. Reports can be emailed to parents if you would like to do so.
      1. You can contact me at a later date to set this up.

**Student Data:** Students' are responsible for their data.

**If a laptop needs to be reimaged for any reason all personal data will be lost. The student needs to take one of the following precautions to prevent loss of documents.**

1. Hard Drive on Computer – will be erased if laptop needs reimaging.
2. Google Drive
3. Network share folder, only accessible while joined to the AISD network.
4. Flash Drive – students may save their documents to an external flash drive.
5. CD Rom – Students may burn to a CD.

## iTunes

Students are not allowed to purchase anything from the iTunes store from their laptop. The school will not be responsible for reimbursing the student for lost purchases from the store after reimaging.

Students may load acceptable music, apps, and other things from their iTunes account.

If unacceptable songs, videos, movies, etc. are found on the laptop it will be reimaged and all information on that computer will be erased.

## Music, Games, or Programs

- Any music downloaded or streamed over the Internet must be **appropriate** as per AISD policy.
- Any games streamed over the Internet must be **appropriate** as per AISD policy.
- Decisions regarding **appropriate** music and games will be at the discretion of the Campus Administration and the AISD Technology Department. All software on the system must be AISD approved and installed by the Technology Department. All copyright laws will be enforced.
- There is a \$15 re-imaging charge to remove any of the above items.

## 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.

## Fair Market Value

Age of Laptop Value:

1. 1 year or less \$ 900.
2. 2 years \$ 700.

- 3. 3 years \$ 550.
  - 4. 4 years \$ 320.
- \* Original cost to the District is currently \$ 1,000.

### Table of Fees, Fines, & Repair Costs

Students are expected to keep the laptops in good condition. Failure to do so will result in the fines as specified below.

- Depending on the specific situation, it will be determined if a student is issued a replacement laptop until theirs is fixed.
- All fines must be paid in full before laptops will be returned/reissued.
- Only components that need to be repaired will be turned in to the repair center. Students are responsible for keeping up with the remaining components.
- In case of theft, a police report must be filed and a copy provided to the technology department. Students will be responsible for the insurance deductible for theft.
- Spot checks of laptops will occur regularly. Students who fail to report damage or abuse will be subject to fines and to discipline.
- “Three strikes, and you’re out” - After the third repair, you are responsible for the full repair cost. (Does not include normal wear & tear repairs.)

### Table of Estimated Repair Pricing

Description of Non-Warranty Repair/ Replacement	Accidental Damage	Deliberate Damage
Broken Screen (LCD)	\$ 100.00	Actual cost of repair
Damaged Keyboard	\$ 100.00	Actual cost of repair
Damaged / Lost Power Supply	\$ 100.00	Actual cost of repair
Damaged / Lost Battery	\$ 100.00	Actual cost of repair
Re-image of Hard Drive	\$ 25.00	Actual cost of repair
Abandonment Fee	\$ 20.00	Actual cost of repair
Other Minor / Major Damage	Up to Cost of Laptop	Actual cost of repair
Replacement Bag	\$0.00 if warranty	\$40.00
Lost / Destroyed Laptop	Fair Market Value	Actual cost of replacement
Theft	\$200 Deductible	

### 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, please contact the campus administration about payment options regarding payment of the fee. Upon proof of financial hardship, the administration may elect to create a payment plan for the student / parent to pay out fees over time.

## **Use of Computers and Laptops on the Network**

Albany ISD is committed to the importance of a student being able to continue with his work when his laptop is experiencing problems.

### **No Loaning or Borrowing Laptops**

- Do NOT loan laptops or other equipment to other students.
- Do NOT borrow a laptop from another student.
- Do NOT share passwords or usernames with others.

### **Classroom Assignments and Websites**

Classes may have online assignments posted on the AISD 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 the District's 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>

### **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 \$25 re-imaging charge. **Re-imaging the laptop will result in the loss of ALL personal data.**

## **Unauthorized Access**

Reference District AUP

## **Transporting Laptops**

- Laptops must be transported in school-provided bags.
- To prevent system damage, laptops need to be closed and placed in school provided bag.
- Laptops do **NOT** have to be shut down (turned off) between classes.
- Laptops 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, laptops, 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.

### **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. Copyright guidelines are on the AISD website.
- c. Although the AISD 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:**

- 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.

- Using the network for financial or commercial gain, advertising, or political lobbying.
- 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.
- 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.
- Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
- Intentionally wasting finite resources, i.e., online time, real-time music.
- Gaining unauthorized access anywhere on the network.
- Revealing the home address or phone number of one's self or another person.
- Invading the privacy of other individuals.
- Using another user's account or password or allowing another user to access your account or password.
- Coaching, helping, observing or joining any unauthorized activity on the network.
- Forwarding/distributing E-mail messages without permission from the author.
- Posting anonymous messages or unlawful information on the system.
- 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.
- Falsifying permission, authorization or identification documents.
- Obtaining copies of, or modifying files, data or passwords belonging to other users on the network.
- Knowingly placing a computer virus on a computer or network.

## Acceptable Use Policy - Albany Independent School District

### A. Electronic Communications & Data Management System:

The Albany ISD Electronic Communications & Data Management System includes:

- Any and all computers owned by Albany ISD, networked or stand-alone.
- Any and all peripherals attached to any network computer including, but not limited to modems, keyboards, monitors, mice, printers, scanners, and digital cameras
- Any and all servers attached to the Albany ISD network
- Any and all network hardware comprising the Albany ISD network



- Any and all computer program software and/or subscriptions licensed to Albany ISD
- Any and all software installed (with Technology Department authorization) on any network or stand-alone computer

### **Network & Internet Services:**

Although Internet access is filtered, it is possible that users may run across areas of adult content and/or material that might be found objectionable.

- Albany ISD will make every effort to educate and guide all Albany ISD network users in the proper use of the Internet; however, it is impossible to control all materials on the global network. Therefore, it is imperative that the user be held accountable for the appropriate utilization of the technology.
- Albany ISD makes no warranties of any kind, whether expressed or implied, for the network service it is providing. The District's system is provided on an "as is, as available" basis. Albany ISD will not be responsible for damages incurred while on this system.
- Albany ISD shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and/or costs incurred by users.
- Albany ISD shall not be responsible for ensuring the accuracy, age appropriateness, and/or usability of any information obtained through its electronic services.

### **User Accounts:**

The Albany ISD network and Internet services are not private.

- The Albany ISD Technology Department and/or Albany ISD administrators may monitor data and/or users at any time to ensure proper use.
- Students in pre-kindergarten through second grades may have system access only through a group account.
- Students in third through twelfth grades will be assigned an individual account for system access.
- Do not share your account or password with anyone.
- Do not allow anyone else to use your account and do not use someone else's account.
- Do not leave your computer unattended. If you must leave your computer for a moment, either log off or lock the computer. Always log off when you are finished.
- The user is responsible at all times for the proper use of his/her account.

### **Network Use and Content:**

- Use of the Albany ISD network must be in support of education and

- research and be consistent with the educational objectives of Albany ISD.
- Use of the Albany ISD Electronic Communications & Data Management System must not interfere with the acceptable use of the network by staff or other students.
  - Users must respect the privacy of others. Users shall not intentionally obtain copies of or modify files or data that belongs to anyone else without permission from the owner of the files/data. Users shall not distribute files or data that belongs to someone else without permission from the owner of the files/data.
  - Albany ISD classes and/or activities often give students the opportunity to have pictures, announcements and/or examples of student work published on the Albany ISD web site. Images will be published without student names or with first names only and work will be given credit by initials or first names only.
  - Students are prohibited from transmitting any material in violation of any United States or other state organizational laws. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret.
  - Students are prohibited from creating or intentionally obtaining files, data and/or E-mail that contains objectionable material. Objectionable material includes, but is not limited to, lewd or foul language or images, materials that are abusive, threatening, harassing or damaging to another's reputation, or information to assist in technology theft or misuse.
  - Students are prohibited from intentionally accessing objectionable material on the Internet. If you unintentionally access objectionable material, you are expected to immediately discontinue the access and report the incident to the supervising teacher or site administrator.
  - For safety reasons, students are not allowed to access or participate in Internet chat rooms, forums, blogs or news groups; except through My Big Campus.
  - Students may not use any sort of Internet or network instant messaging program.
  - Forgery or attempted forgery of Email messages and/or data is prohibited. Do not attempt to read, delete, copy, or modify the E-mail and/or data of other network users.
  - Plagiarism and cheating using technology is prohibited.

### **Computer Systems:**

- Students are prohibited from downloading and/or installing files or software unless permission is granted by the Albany ISD Technology Department. All users must respect the legal protection provided by copyright license to programs, books, articles and data. Installation of unlicensed software will not be permitted under any circumstance.
- Students are allowed to use specific external data storage system CD's,

- Flash drives and saving to the space provided by My Big Campus.
- Students shall not attempt to write, produce, generate, copy, propagate or introduce any computer code designed to self-replicate, damage, change or otherwise hinder the performance of any computer's memory, file system, or software. Such software is known as a bug, virus, worm, Trojan, or similar name.
  - Vandalism is defined as any malicious attempt to harm or destroy any equipment and/or data of another user or of any other networks that are connected to the system. Deliberate attempts to degrade and/or disrupt system performance are violations of District policy and may constitute criminal activity under applicable state and federal laws. Any vandalism will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

### **Inappropriate Use:**

The use of the Albany ISD network and Internet services is a privilege, and inappropriate use will result in cancellation or suspension of this privilege and/or disciplinary action in accordance with District policies and the Student Code of Conduct. Albany ISD administration will rule upon inappropriate use.

- Possible Consequences of Inappropriate Use:
  - Suspension of user access to the system
  - Termination/Revocation of the system user account
  - Other disciplinary or legal action, in accordance with district policy and applicable laws.

### **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.

#### **D. E-Mail**

*(Student e-mail is in the developmental process and will be addressed at a later date.)*

- 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 laptop are property of the District.
- Unauthorized use of another individual's 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:**

- Sending chain letters;*
- Sending copies of documents in violation of copyright laws;*
- Forwarding email 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;*
- Sending messages that have restricted access due to federal, state, or District regulations; or*
- Sending 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 Albany 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
- Albany 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 Albany 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.

### **Technology Offenses and Disciplinary Actions**

The student in whose name a system account and/or computer hardware issued will be responsible at all times for its appropriate care and use.

Noncompliance with the guidelines published in the Student Code of Conduct and in Board Policy may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to Level III Technology Discipline Offense of the Code of Conduct. Violation of applicable state or federal law, including the Texas Penal Code, Computer Crimes, and Chapter 33 will result in criminal prosecution or disciplinary action by the District. Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. The District cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of email and network communications are governed by the Texas Open Records Act; proper authorities will be given access to their content.

### **Level I Technology Offense**

***Reference Student Code of Conduct***

**Level II Technology Offense** Level II Technology Offenses are more severe and/or more persistent than Level I Technology Offense. The student's conduct infringes upon the rights of other students or adults. The student's conduct negatively impacts the educational efficiency of other students and the staff. The administrator who is working with the student may invite the parents to participate in a conference in order to review

Level I procedures that have been attempted, to solicit their cooperation in changing the student's behavior, and to inform them of the serious consequences of persistent Level II Technology Offense:

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

**Level II Technology Disciplinary Action** Consequences of Level II Technology Disciplinary Actions include, but are not limited to, the following:

1. Any Level I Technology Disciplinary Action or combination of disciplinary actions.
2. In-school suspension.
3. Suspension.
4. Notification of outside agency and/or police with filing of charges when appropriate.
5. Behavior contract.
6. Behavior improvement parent involvement program.
7. Voluntary enrollment in a residential rehabilitation/treatment program.
8. Assignment to disciplinary alternative education program.

**Level III Technology Offense** Level III Technology Offenses 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 Level III Technology Offenses include, but are not limited to, the following offenses committed on school laptop or within 300 feet of school property, or while attending a school-sponsored or school-related activity except as noted:

9. Engages in conduct that contains the element of breaching computer security under Section 33.02(b)(2-5) of the Texas Penal Code.

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

**Level III Technology Disciplinary Action** Consequences of Level III Technology

Disciplinary Actions include, but are not limited to, any of the following: The consequences of Level II Technology Offenses 1-10 may result in an assignment to a disciplinary alternative education program.

**Consequences for Level III Technology Offenses may also include the following:**

1. Notification of police, with filing of charges when appropriate.
2. Permanent removal from the class of the teacher reporting the offense.
3. Voluntary enrollment in a residential rehabilitation/treatment program.
4. Withdrawal of various privileges (computer access).

## Texas Penal Code

### 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) 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:
  - 1) a Class A misdemeanor if the aggregate amount involved is less than \$1,500
  - 2) a state jail felony if the aggregate amount involved is \$1,500 or more but less than \$20,000;
- c) or the aggregate amount involved is less than \$1,500 and the defendant has been previously convicted two or more times of an offense under this chapter;
- d) a felony of the third degree if the aggregate amount involved is \$20,000 or

- more but less than \$100,000
- e) a felony of the second degree if the aggregate amount involved is \$100,000 or more but less than \$200,000; or
- f) a felony of the first degree if the aggregate amount involved is \$200,000 or more.

A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

## Internet Safety Tips for Parents

### Online tips for parents:

**LOCATION:** The MacBook 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 MacBook 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 e-mail. 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 who 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>

## **Student Expectations for MacBook Use**

I will take good care of my MacBook and understand I will be issued the same MacBook each year.

1. I will never leave my MacBook unattended.
2. I will never loan out my MacBook to other individuals.
3. I will know where my MacBook is at all times.
4. I will charge my MacBook's battery daily.
5. I will keep food and beverages away from my MacBook since they may cause damage to the computer.
6. I will not disassemble any part of my MacBook or attempt any repairs.
7. I will protect my MacBook by only carrying it while in the carrying case provided by the district.
8. I will only use my MacBook in ways that are appropriate and educational.
9. I understand that my MacBook is subject to inspection at any time without notice and remains the property of Albany ISD.
10. I will follow the policies outlined in Albany ISD's Acceptable Use Policy while at school and any other place I use my MacBook.
11. I will file a police report in case of theft, vandalism, and other acts covered by insurance.
12. I will be responsible for all damage or loss caused by neglect or abuse.
13. I agree to pay for the replacement of power cords, battery, or MacBook case in the event any of these items are lost or stolen.
14. I agree to return the District MacBook and power cords in good working condition immediately upon request by the District.