

## **ACCEPTABLE USE FOR TECHNOLOGY AND NETWORK RESOURCES**

Technology and network resources are valuable tools for students, staff, and community. The Appleton Area School District (AASD) provides computer facilities, equipment, software and a local and wide-area network that is accessible for the primary purpose of supporting the educational mission of the District. The District's technology system includes, but is not limited to: desktop and portable computers; voice over internet protocol phone system; file, web, and print servers; projection devices; software applications; electronic devices such as cell phones, pagers, personal digital assistants; the internet; and voice messages. Unless otherwise specified, the following regulation shall apply equally to all AASD users including employees, contractors employed by the AASD, students, volunteers, and guests. The AASD permits users to connect to the District network with personal computing devices following acceptance of user agreement terms. Users may have additional obligations given the nature of their positions and/or access privileges.

Use of the District technology system is a privilege and not a right. Users of the District's system should have no expectation of privacy in the content of their personal files, communications, and records of their online activity. The AASD reserves the right to monitor, access, delete and/or disclose all files, communications, and use of the District's technology system at all times without user permission within legal parameters.

It is the responsibility of users to provide for the reasonable care of all District technology. The AASD reserves the right to hold users accountable for vandalism, misuse, and damage to the system in violation of the rules outlined in this policy, including revoking privileges, taking disciplinary and/or legal action. All users must have an appropriate "User Agreement" with the District to access the technology system (Appendix A).

The use of the AASD Student Information System (SIS) is solely for the purpose of facilitating the exchange of information to further communication, education, and research consistent with the mission of the AASD. The SIS and the communications transmitted and documents created on it are the property of the District. The AASD reserves the right to supervise the use of such property. Each user requesting access to the SIS must contact the AASD Technology Services Department

### **A. NETWORK GUIDELINES**

### **B. ELECTRONIC COMMUNICATIONS GUIDELINES**

### **C. SOFTWARE GUIDELINES**

### **D. WEB PUBLISHING GUIDELINES**

### **E. PRIVACY GUIDELINES**

### **F. PROHIBITIONS AGAINST DISCRIMINATION, HARASSMENT, BULLYING, AND DEFAMATION**

### **G. COPYRIGHT GUIDELINES**

### **H. SOCIAL MEDIA GUIDELINES**

### **I. MONITORING, SUPERVISION, AND CONSEQUENCES**

### **J. PERSONAL TECHNOLOGY USE IN SCHOOL**

1. Bring Your Own Device
2. One-to One (1:1) Device Program

**Adoption Date: July 16, 2001**

**Amended Date: May 22, 2006, August 27, 2012, May 28, 2013, and  
October 27, 2014; November 23, 2020**

## **ACCEPTABLE USE FOR TECHNOLOGY AND NETWORK RESOURCES**

### **Procedures**

#### **A. NETWORK GUIDELINES**

The Appleton Area School District (AASD) maintains a local and wide-area network that links schools together and also provides access to public networks. This network consists of a hard wired and wireless network. The wireless network includes, but is not limited to, the District-provided wireless access and any other wireless data provider (e.g., cell phone or personal wireless hotspot) used on any AASD property and its school campuses. The purpose of the AASD network is to facilitate the exchange of information to further communication, education, and research consistent with the educational mission of the AASD. Users are responsible for their actions/behavior and communication on the network in order to maintain a safe, lawful, and efficient network.

Network use or attempted use that is unacceptable at all times includes, but is not limited to:

- accessing the network for illegal activity, political or religious purposes, and unethical or disruptive activity.
- placing unlawful information on the network.
- accessing inappropriate content, including pornographic or obscene items.
- disrupting network traffic, overloading or crashing the network and attached systems.
- monitoring or capturing network traffic in any way.
- gaining unauthorized access to information resources or accessing, changing, deleting, or damaging another person's materials, information, or files.
- installing or running a program which damages or places an excessive load on technology and network resources.
- wasting or stealing consumables (e.g., paper, toner, storage devices) associated with the network system.
- disrupting the educational environment with District or personal computing devices.
- accessing or sending offensive or objectionable material to others.
- cyberbullying.

The AASD places a high priority on the security of its technology and network resources. The District has systems in place that can monitor and record all network usage. It scans all inbound and outbound emails, plus attachments, for viruses, but does NOT guarantee such messages to be virus-free. The AASD accepts no responsibility for any damage caused by sending or receiving messages through the electronic communications system. The Technology Services Department may create filters to scan for and eliminate viruses and large graphic files that are unrelated to the District's educational mission.

Users must be responsible for taking security precautions when accessing the District's technology and network resources. Use that is unacceptable at all times includes, but is not limited to:

## **363-Rule (cont.) (522.7-Rule)**

- not taking reasonable measures to prevent others from using identifying information.
- sharing accounts or leaving accounts open or unattended.
- not keeping all accounts and passwords confidential and inaccessible to others.
- not respecting the rights and property of others and improperly accessing, misappropriating, or misusing the files, data, or information of others.
- not making backup copies of documents critical to the user.
- not taking precautions to prevent viruses, spyware, and malware on personal and District devices.
- gaining unauthorized access, altering, deleting, damaging, or destroying any network, program, or data.
- not reporting unusual activity such as spam and phishing schemes to the AASD Helpdesk.

### **B. ELECTRONIC COMMUNICATION GUIDELINES**

Use of the AASD electronic communication systems is provided to students and staff to further the educational mission of the AASD. These electronic communication systems include, but are not limited to: email, blogs, social media, learning management systems, telecommunication systems, and other web-based/electronic tools. Interpretation of appropriate use of electronic communication is the responsibility of the AASD Administrative Leadership Team. The Technology Services Department is responsible to ensure the efficient use of the District technology system.

AASD employees:

- are required to check email and other District-provided online communications because they are the official means of communication and business for the District.
- may have use of email for personal reasons, as long as it conforms to school etiquette standards and is not used excessively.
- may have limited use of the District communication systems for personal business interests including private or commercial offerings of products or services or to solicit products or services on designated District web pages.

AASD students:

- may use the District communication systems for contact with school employees, access to outside resources related to school assignments, and student collaboration on school activities.
- may only receive emails on the network from District employees, other AASD students, and persons that have been approved by the District. Unauthorized emails will be blocked and returned to the sender.
- will have their accounts removed from the systems after graduation or withdrawal from the District.

AASD employees and students will:

- delete unwanted emails immediately and keep them to a minimum in order to maximize District storage resources.
- not use e-mail for chain letters or other mass solicitations.
- report technical issues related to email accounts and electronic communications to the AASD Helpdesk.

### **C. SOFTWARE GUIDELINES**

All District online resources, including software purchased or acquired for educational use, will be approved by the Assessment, Curriculum and Instruction Department (ACI) and installed by the Technology Services Department.

### **D. WEB PUBLISHING GUIDELINES**

The AASD believes that certain guidelines must be followed when creating school web pages in order to maintain high standards. Guidelines are intended to provide direction, consistency, and integrity to maximize accessibility. Guidelines are not an attempt to limit creativity.

Guidelines that apply to school web pages include, but are not limited to, the following:

- First and/or last name of a student may only be published with permission from parent(s)/guardian(s).
- Created web pages may not contain copyrighted material without proper permission.
- All District, department, and school-published web pages will include a copyright notice.
- Parent(s)/guardian(s) may opt out of having pictures, videos, or the name of their student(s) posted or identified on District/School created web pages.
- Student users who create web pages should clearly identify web pages as student-created and that the students' opinions are not necessarily a reflection of the AASD.
- Created web pages may not contain confidential information or information that is in violation of state or federal laws or Board policy.
- Links will be limited only to provide educational information about other youth activities, agencies, or organizations that are known to be nonsectarian, nondiscriminatory, and devoted to school/community interests or child welfare.
- The user that creates a web page that is linked to the AASD homepage is ultimately responsible for the content including links. The AASD reserves the right to review and approve the pages.
- The principal/supervisor of each school site or manager of each department is responsible for compliance with guidelines.

### **E. PRIVACY GUIDELINES**

AASD network users should have no expectation of privacy in the content of their personal files, communication, or their online activity while using the District's technology system. Network content including, but not limited to, documents and other communication may be considered public and subject to disclosure. The AASD reserves the right to retrieve contents and user files on its system for legitimate reasons including, but not limited to: finding lost messages, conducting internal investigations, complying with open records requests, investigating wrongful acts, or recovery from system failure.

The District also reserves the right to retrieve contents and user files to conduct student investigations relating to suspension and/or expulsion and personnel investigations relating to discipline and/or termination.

## **363-Rule (cont.) (522.7-Rule)**

The use of the AASD Student Information System (SIS) is solely for the purpose of facilitating the exchange of information to further communication, education, and research consistent with the mission of the AASD. The SIS and the communications transmitted and documents created on it are the property of the District. The AASD reserves the right to supervise the use of such property. Each user requesting access to the SIS must contact the AASD Technology Services Department. Student records and communication between students or family and staff are protected by the Family Educational Right to Privacy Act (FERPA).

Users must be responsible for their own privacy and personal safety as well as that of others when using the District's network. Use that is unacceptable at all times includes, but is not limited to:

- violating the privacy rights of self/others by providing home address, telephone number, or other personal information.
- recording of any type including, but not limited to: audio, video, images, and photographs, in violation of Board Policy 492-Photographing and Videotaping in the Schools.

### **F. PROHIBITIONS AGAINST DISCRIMINATION, HARASSMENT, BULLYING, AND DEFAMATION**

The District has an obligation to provide a school environment free of discrimination, harassment, bullying, and defamation. Users of the District's technology must comply with state and federal laws and Board policy regarding these items. Use that is unacceptable at all times includes, but is not limited to:

- accessing, displaying, or sending messages and materials that use language, audio or images that are discriminating, harassing, bullying, or defaming.
- circumventing District content filters in order to access the content listed above.

### **G. COPYRIGHT GUIDELINES**

The AASD recognizes and supports the limitation imposed by copyright laws. These laws specifically prohibit unauthorized duplication of software and online resources except to provide for archival back-up copies. The AASD declares it to be inappropriate to use "pirated" or otherwise illegally obtained software or protected online resources on the District systems. The use of District technology equipment or systems to make unauthorized copies of District-owned, privately-owned, or illegally obtained software or protected online resources is prohibited.

Copyrighted material may not be posted on any District website or used as an attachment or link without permission from the creator. Reproduction or use of copyrighted materials will be done either with the written permission of the copyright holder or within the bounds of the "fair use" guidelines provided in the copyright law under Title 17 of the United States Code (i.e. "in-house" productions, un-copyrighted works, or works in the public domain); otherwise, the user responsible for reproduction or use may be liable for breach of copyright under existing laws.

The principal/supervisor of each school site or manager of each department is responsible for compliance with copyright law.

## **H. SOCIAL MEDIA**

Social media is defined as “online services that require communication between two or more people” and encompasses a wide range of written, audio, and visual communication. Social media networks include, but are not limited to: personal websites, blogs, wikis, social networks, online forums, twitter, and virtual worlds.

The District recognizes the importance of online social media networks as a communication and learning tool for AASD staff and students. The District also recognizes its obligation to teach and ensure responsible and safe use of these technologies. Toward that end, the District provides password-protected social media tools and District-approved technologies for e-learning and encourages the use of District tools for collaboration by employees and students.

Public social media networks are generally available to the public or consumers and are not provided by the District’s electronic technologies network. Public social media networks include, but are not limited to: Facebook, Twitter, YouTube, and blog sites. The District takes no position on AASD employees’ decision to participate in the use of public social media networks for solely personal use on personal time. However, AASD employee use of these media that exist outside of those approved by the District during school hours is prohibited unless given special permission by administrators or the Technology Services Department.

All employees are expected to serve as positive ambassadors for our schools and are role models to students in the community. Readers of social media networks may view the employee as a representative of schools and the District. Therefore, the AASD requires employees, when referring to the District, its schools, students, programs, activities, employees, coaches, advisors, volunteers, and communities on any public or District-approved social media networks to observe the following requirements that include, but are not limited to:

- Use of any social media network or postings, displays, or communications on any social media network must comply with all state and federal laws and District policies.
- Communications by word, image, or other means must be respectful and professional.
- Authorized spokespersons for the District must disclose their employment relationship with the District.

Confidential or proprietary information of the District, its students, or employees or that which is protected by data privacy laws may not be disclosed.

- The AASD name or its logo may not be posted or used without permission from the Superintendent or his/her designee.
- No images of co-workers may be posted without the co-workers’ consent.
- Unless parents have opted out of having pictures, videos, or the name of their student(s) posted or identified on District/School created web pages, images may be posted, including images of students taken in the public arena.
- No nonpublic images of the District premises and property, including floor plans, may be posted.

## **363-Rule (cont.) (522.7-Rule)**

- Engagement with student groups that are within the District or in the public must be as a District-employee maintaining appropriate employee-student relationships and addressing inappropriate behavior or activity on the networks, including protecting the safety of minors online.
- District information posted to a social media personal profile must be limited, but may include District employment information including, District name, job title and duties, status updates on job promotion, and personal participation in District-sponsored events, including volunteer activities.
- Employees and adults working on behalf of the AASD (e.g. student and substitute teachers, interns, volunteers) must treat student images and information with confidentiality in accordance with AASD Policy 492, Photographing and Videotaping in the Schools.
- Purposeful or inadvertent disclosure of confidential or private information that violates the privacy rights or other rights of a third party, or the content of anything posted on any social media network is the responsibility of the employee.

AASD student use of social media during instructional time will be limited to educational purposes.

Any users of social media on the AASD network must adhere to the guidelines listed in this policy and its procedures.

The AASD may use social media networks and other communication technologies in fulfilling its responsibility for effectively communicating with the general public.

### **I. MONITORING, SUPERVISION, CONSEQUENCES**

The AASD Technology Services Department has systems in place that can monitor and record all network use for consistency in enforcing technology and network protocols. The District provides instruction for employees on the appropriate and inappropriate use of its technology systems and requires employees to supervise students' usage of District and personal computing devices. The District provides instruction for students on the appropriate and inappropriate use of its technology and network resources in the classroom.

To reduce the risk of compromising District resource security, it is important that all users assist in reporting any inappropriate usage, including, but not limited to hacking, inappropriate content, phishing, and spamming to employees, administrators, the Helpdesk, or Technology Services Department.

All volunteer, guest, and contractor users must accept the "User Agreement" by clicking the accept box on the device screen before gaining access to the District network (See Appendix A).

Consequences for violations of the Acceptable Use of Technology and Network Resources Policy and Procedures may result in the suspension/revocation of technology privileges, discipline up to and including suspension and/or expulsion for students, and discipline up to and including termination for employees. The District will investigate and report unlawful activities to authorities.



Appeals may be made in accordance with appropriate Board policies, procedures, and employee and student handbooks.

## **J. PERSONAL COMPUTING DEVICE USE IN SCHOOL**

### **1. Bring Your Own Device**

#### **Personal Computing Devices/BYOD**

Families may choose to use personal computing devices for instructional use in place of a District-assigned device. The AASD is not liable for damage, loss, theft, or IT issues of personal computing devices. Students who choose to bring their own personal computing device do not rescind the District's right to inspect the computing device at any time while on school property based on legal authority. The AASD does not guarantee support for download tools to personal computing devices, including links, applications, and extensions. (Appendix B)

The AASD provides a community accessible network with the primary purpose of supporting the educational mission of the District. The District permits AASD students, with parent/guardian permission, to bring personal computing devices to school for the purpose of connecting to District network resources (Appendix B).

The use of personal computing devices in the District is a privilege, not a right. Ensuring its proper use is the joint responsibility of students, parents, and employees with the following liabilities and limitations including, but not limited to:

- AASD students must have a signed permission form from their parent(s)/guardian(s) on file for use during the school day (Appendix B).
- Student use of personal computing devices during instructional time may be limited at the discretion of the teacher.
- Network access is provided on an "as is, as available" basis.
- The District is not responsible for delays, changes, or interruptions of communication or internet service, regardless of the cause.
- The District assumes no financial obligations arising through use of the AASD network.
- The AASD is not responsible for damage caused by inappropriate or inadvertent activity due to interaction with the network.
- The AASD is not responsible for damages to, loss of, or theft of personal computing devices. The District will investigate and refer unlawful acts to authorities.
- The AASD will not provide technical support for personal computing devices.
- Any damage to AASD technology or property due to the unauthorized use of personal computing devices will become the liability of the owner of the device.
- Administrators and professionals may confiscate personal computing devices while on District property if they have reasonable suspicion that the use of these items is in violation of policy or disruptive to the educational environment.
- Confiscated personal computing devices may be subject to search.

**363-Rule (cont.)  
(522.7-Rule)**

Acceptable uses of personal computing devices are those which support the educational mission of the AASD. Users are subject to all of the guidelines of this policy and its procedures. Use of personal computing devices that is unacceptable at all times includes, but is not limited to:

- physically connecting personal computing devices to the AASD wired network.
- tampering with, damaging, or modifying District technology with the use of a personal computing device.
- using personal computing devices in such a way as to disrupt the use of District technology by other users.
- disrupting any educational environment including, but not limited to: classes, study hall, library, assemblies, field trips, and co-curricular activities.

**2. One-to One (1:1) Device Program**

The AASD is loaning all students in grades EC-12 a computing device for educational purposes during the academic year. The AASD will hold the legal title to the computing device and all accessories. Right of possession and use is limited to and conditioned upon full and complete compliance with all AASD student school handbooks and Board policies and procedures including, but not limited to: 363, 443.5, 492, and 443.92. The AASD does not guarantee that its technology resources will be uninterrupted or error-free. Access to the network is provided on an “as is” basis without warranties of any kind. In the event that the network is down, neither the AASD, nor any of its agents or employees will be responsible for lost or missing data.

The right to use and possess the computing device and its peripherals will terminate annually no later than the last day of the school year, unless terminated earlier by the District or upon removal from the District through withdrawal, suspension, expulsion, or transfer to another district; or terminated later due to a District determined need . Failure to return the device on or before this date may result in criminal charges being sought against the student, parent/guardian, or the person in possession of the computing device. The computing device remains the property of the AASD and cannot be loaned, sold, bartered, traded, leased, rented, or given to any other person(s). Failure to return the computing device and peripherals may result in a certified letter sent to the parent/guardian or adult student requesting return of the missing computing device. The parent/guardian or adult student will have five (5) days to return the items or pay replacement costs. Failure to comply will be referred to local law enforcement. The parent/guardian or adult student may be charged with theft. The AASD reserves the right at any time to require the return of the computing device. Students may be subject to loss of privileges, disciplinary action and/or legal action in the event of damage to or loss of the computing device or violation of AASD Board policies and guidelines.

**Modifications to the Program**

The AASD reserves the right to revoke or modify the one - to - one (1:1) program and/or its policies and procedures at any time.

## **363-Rule (cont.) (522.7-Rule)**

### **District Liability**

The AASD assumes no liability for any material accessed on the computing device.

### **Monitoring Usage**

The AASD has installed software on its computing devices to facilitate in the monitoring of student internet usage. While the AASD is committed to protecting students, no technical or human supervision is fail-safe. The AASD reserves the right to investigate, review, monitor, and restrict information stored and transmitted on District-owned devices. Any attempt by students to circumvent the monitoring and filtering systems in place including, but not limited to, resetting the device or attempting to install or use proxy servers, will result in disciplinary action. This action may result in loss of student use of the device and/or other consequences deemed appropriate by AASD administration up to, and including, expulsion.

### **Damaged/Lost/Stolen Computing Devices**

Computing devices in EC-6 are assigned to school at the ratio of 1 device per student. Computing devices for students in grades EC-6 will be restricted to on campus student use unless directed by school or district administration to be brought home. Computing devices in grades 7-12 are assigned to students in a similar fashion and process as assigning textbooks. However, unlike textbook assignment, each student will be assigned the same device each year in grades 7 and 8. Students will be assigned a new device in grade 9 and that device will remain with that student for the duration of the student's AASD high school career. It is understood that as materials are used, normal wear is expected. What is not expected is damage that is above what is considered normal wear. As with textbooks, students may be issued a fine at the end of the school year if excessive wear or damage is evident.

It is also understood that when using electronic devices, damage may occur. There are three types of damage to school property: accidental, negligent or malicious. If a device is damaged, the student must return it to the school's designated helpdesk to generate a repair order and to determine if the damage was accidental or malicious/negligent. If device damage is determined to be accidental, the student may be able to check out a loaner while the device is being repaired. The student will not be charged for the repair. If a device is damaged through malice or negligence, the student will be responsible for all repair costs. The student may qualify to use a computing device for use during the school day that is restricted to school campus use. In addition, students may face administrative or legal consequences depending on the nature of the damage.

If the device is lost or stolen, the student must notify school administration immediately. Administration will make contact with the Police School Liaison (PSL) to generate a police report. Efforts will be made to find and return the device. If recovery efforts are unsuccessful, the parent/guardian or adult student may be responsible for reimbursing the District up to the device's full replacement cost. The student would not be required to reimburse the District for the cost of warranty or setup charge. A student with a lost or stolen device who fails to notify school officials in a timely fashion may be subject to disciplinary action.

**363-Rule (cont.)  
(522.7-Rule)**

**Consequences**

Consequences for non-compliance with District policy as well as procedures in the handbook include disciplinary actions and financial responsibilities. Any failure to comply with policy may immediately end the student's right to access the computing device, or other devices or services. The student may also be subject to disciplinary action as set forth in the school's student handbooks and AASD Board policy. The AASD cooperates fully with local, state, and federal law enforcement in the investigation of all computer-related crimes.

**Cross References: Internet Safety Policy (CIPA), 363.2  
Photographing and Videotaping in the Schools, 492-Rule  
Violence and Intimidation, 443.7  
Bullying Policy, 443.71  
Locker Room Privacy, 443.92**

**Legal References: Wisconsin State Statutes 120.12, 943.7, and 947.0125**

**Adoption Date: July 16, 2001**

**Amended Date: May 22, 2006, August 27, 2012, May 28, 2013, and  
October 27, 2014; November 23, 2020**

## **Appendix A - Board Policy 363, 522.7 General Public Acceptable Use Policy Agreement**

*The following conditions must be agreed to by clicking accept on this entry screen before accessing the District network and its resources.*

The school's information technology resources, including email and Internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to the school's technological resources.

### Users must:

1. Respect and protect the privacy of others.
  - Use only assigned accounts.
  - Not view, use, or copy passwords, data, or networks to which they are not authorized.
  - Not distribute private information about others or themselves.
2. Respect and protect the integrity, availability, and security of all electronic resources.
  - Observe all network security practices, as posted.
  - Report security risks or violations to a teacher or network administrator.
  - Not destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner.
  - Conserve, protect, and share these resources with other students and Internet users.
3. Respect and protect the intellectual property of others.
  - Not infringe copyrights (no making illegal copies of music, games, or movies!).
  - Not plagiarize.
4. Respect and practice the principles of community.
  - Communicate only in ways that are kind and respectful.
  - Report threatening or discomfoting materials to a teacher.
  - Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
  - Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
  - Not use the resources to further other acts that are criminal or violate the school's code of conduct.
  - Not send spam, chain letters, or other mass unsolicited mailings.
  - Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

### Consequences for Violation:

Violations of these rules may result in disciplinary action, including the loss of a student's privileges to use the school's information technology resources.

### Supervision and Monitoring:

School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

**Appendix B - Board Policy 363, 522.7  
Student Bring Your Own Device (1:1 Opt Out)  
Acknowledgment of Student Responsibilities**

Student Name \_\_\_\_\_

Personal computing devices will be allowed on the AASD network for instructional use. The AASD is not liable for damage, loss, theft, or IT issues of personal computing devices. Students who choose to bring their personal computing device do not rescind the District's right to inspect the device at any time while on school property based on legal authority. The AASD does not guarantee support for installed tools on personal computing devices.

When electing to use a personal computing device in lieu of accepting a District-owned device, the following student responsibilities must be acknowledged:

- Any personal computing device should have the ability to hold at least 6 hours of battery life during normal use. Charging stations for personal computing devices will not be available on campus.
- While AASD is not endorsing a specific model of personal computing device, any personal computing device used as the primary computing device on campus should have the latest version of the Chrome Browser installed and be allowed to install AASD-requested Chrome apps and extensions.
- Personal computing devices may not be allowed for use during administration of certain classroom, building, District, State, Federal, or other online assessments and may require use of a District-owned device.

Smart phones, mini-tablets, and other web-enabled handheld devices inherently possess certain limitations. While use of these devices is not explicitly forbidden, such a device should not be the sole device for instructional use during the school day.

**Please indicate your personal device make and model  
(example: Make=Samsung      Model=Galaxy Tablet)**

Make \_\_\_\_\_ Model \_\_\_\_\_

I HAVE READ AND UNDERSTAND THIS DOCUMENT AND AM ACKNOWLEDGING THAT MY CHILD WILL NOT BE ACCEPTING A DISTRICT-ISSUED CHROMEBOOK AT THIS TIME

Parent /Guardian Name \_\_\_\_\_ Date: \_\_\_\_\_

Parent /Guardian Signature \_\_\_\_\_