NETWORK AND INTERNET ACCEPTABLE USE AGREEMENT

The Altus Public Schools Instructional Resources Policy and accompanying Regulations will govern all of the District's computer systems and Internet services accessed by all technology users. The term "Users," refers to all technology users and is defined as all staff, students, and individuals provided access to the network. Users will comply with current requirements regarding the responsible use of the system and network.

Altus Public Schools recognizes that as technologies evolve, the manner in which information may be accessed, communicated, and transferred may alter teaching and learning practices. It is the District's intent to provide reasonable, equitable, and safe access to and storage of information for both employees and students. As in all of its work with and for students and families, the Family Educational Rights and Privacy Act (FERPA), the Child Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA), and other federal and state laws guide many of the District's decisions with regard to the wise and judicious use of technology.

Users of the network will respect and comply at all times with local, state, federal, and international laws governing or relating to their use of the network. The District will cooperate fully with local, state, federal, and international officials in any investigation concerning or conditions of the Network and Internet Acceptable Use Agreement understands the policies, and agrees to abide by all terms and conditions described in the agreement or subsequently implemented by Altus Public Schools.

Network and Internet Access - Terms and Conditions.

1. **Acceptable Use:** The use of District-owned devices, networks, and Internet systems must be in support of education and consistent with the educational objectives of the District. The transmission of any material in violation of any United States or state law or regulation is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or material protected by trade secret. The use of the District system for commercial activities is not acceptable. Use for product advertisement or political lobbying is also prohibited. All documents, images, and communication created and/or stored on a District computer or server are considered public under the Oklahoma Open Records Act.

2. **Parental Consent:** By signing the Network and Internet Acceptable Use Agreement a parent is requesting that their child be granted Internet access under the terms and conditions described in this agreement. Parents may withdraw their consent at any time. Parents may revoke all or partial access to technology for their child at any time, with the exception of state-mandated online testing, and may do so by contacting site-level administration. Every accommodation possible will be made to restrict access to

technology upon parent request and will be individualized per situation to best meet the needs of each family.

3. **Privilege of Use:** District Network and Internet access is a privilege. Use of these resources is not a right and inappropriate use will result in appropriate consequences as mentioned above. Inappropriate use is any use prohibited by the terms of this agreement, Board of Education policy, or use determined by the District's system administrators to be inappropriate.

4. **Inappropriate Use:** Each system user is expected to comply with all District policies governing Network and Internet access and to abide by the generally accepted rules of network etiquette. These general rules include, but are not limited to, the following:

a. Appropriate language: Do not use abusive language in messages to others. Be polite. Do not use obscene or profane language, vulgarities, and rude or disrespectful language. Do not engage in personal attacks or activities intended to distress or annoy another user.

b. Safety: Students will be educated about safe and appropriate online behavior, including interactions with other individuals on email, messaging, and social networking websites in an effort to assure their safe and secure use of direct electronic communications on the District network. In addition, cyberbullying awareness and response will be addressed in student handbooks and classroom instruction.

c. Email: Users should be aware that email is not private communication.

d. Network resources: Students should not use the network in a way that will disrupt the use of the network by other users (examples include but are not limited to: sharing apps, apps that circumvent filters or restrictions, executable programs not authorized by APS). The network should be used for educational activities only and should refrain from downloading large files (20MB or larger) unless absolutely necessary. The downloading of hacking or sniffing software will result in the immediate loss of District network and Internet access.

e. Intellectual property: Do not plagiarize works obtained from the Network and/or Internet. Users must respect the rights of copyright owners and comply with all limitations imposed upon the use of copyrighted material.

f. Inappropriate materials: If a user inadvertently accesses inappropriate material, or has knowledge of others accessing inappropriate material, the user should immediately inform an administrator and complete an incident report. The administrator shall investigate, take appropriate action, and notify the involved parties.

5. **Limitation of Liability:** To comply with the Child Internet Protection Act (CIPA) and other federal and state statutes, the School District will utilize filtering software or other technologies to protect users from accessing visual depictions that are obscene, pornographic, or harmful to minors. However, it is impossible to guarantee that students will not be exposed to inappropriate material through their use of the Internet. The District believes that parents bear primary responsibility for communicating acceptable behavior and family values to their children. The District encourages parents to discuss with their children what material is and is not acceptable for their children to access through the District system. Parents of children may request an individualized browsing history report through the Technology Services Center. Parents may revoke access to technology for their child at any time and may do so by contacting site-level administration. These restrictions will be individualized per situation to best meet the needs of each family. Every accommodation possible will be made to restrict access to technology upon parent request.

6. **Security:** Users are responsible for their individual accounts and should take precautions to prevent others from accessing that account. Under no conditions should a user provide their personal password to another person. If you identify a potential security problem on the District system or the Internet you must notify an administrator immediately. For the protection and security of Altus Public Schools' networked

system, it is prohibited to directly attach any network device, such as a wireless access point, to the Altus Public Schools' network or to create a personal wireless network while on campus.
7. **Vandalism:** Vandalism is defined as any malicious attempt to harm or destroy the property or data of the District, or another user and is strictly prohibited. Students will be responsible for the safe, responsible, and appropriate use of the devices at all times. Destruction, theft, loss, and other forms of malice against APS iPads, Chromebooks, and accessories are subject to fees and costs to be paid by the student and/or the student's guardians. The fees and costs are listed in Section 17 of this document.
8. **Social Networking:** Using social networking or messaging sites in a manner that distracts from or disrupts the educational process is prohibited.
9. **Data Collection:** Altus Public School District uses several computer software applications and web-based services operated by third parties. The District assumes parental permission allowing the school to act as an agent for parents in order to comply with the Children's Online Privacy Protection Act (COPPA). If you wish to revoke the District's permission, visit your site-level administrator. These restrictions will be individualized per situation to best meet the needs of each family. Every accommodation possible will be made to restrict access to technology upon parent request.
10. **Application Usage:** Applications for use for instructional purposes are provided by the District through the JAMF Student Application located on each device. These apps have been researched for instructional purposes, and collect no or minimal personal data from the end user. Any apps downloaded outside the App are not authorized by Altus Public Schools to be used in instructional settings.
11. **Personal Devices:** Personal computing devices are permitted, as long as all District and site rules and procedures are followed. Personal computing devices will not be supported by the District. Students who choose to bring personal devices to school do so at their own risk. Altus Public Schools is not responsible for the theft or loss of personal wireless devices. Personal data, images, other media, or software may be removed from District technology at the discretion of the District, as required to properly maintain District resources.

12. **Cell Phones:**

📷 Cell phones and personal devices should not serve as distractions from instruction or learning.

📷 Principals or teachers may determine circumstances wherein the use of such devices may contribute to and facilitate the learning process (examples include but are not limited to text-to-speech apps, online library apps not available on other devices, apps specific to the unique needs of a student defined in an individualized education plan).

📷 The use of personal devices and cell phones should never be a required component of classroom instruction or extracurricular activities.

📷 Inappropriate student use of personal devices and cell phones on school property, in District vehicles, or during school-sponsored activities, is subject to District discipline and acceptable use policies.

📷 Teachers should not ask students to download unauthorized applications.

📷 **Elementary** - Cell phones and other personal devices should be powered off and stored in a designated space.

📷 **Middle School** - Cell phones and other personal devices should be silenced and put away during the instructional day. Cell phones should not be used during passing or lunch/recess times.

📷 **High School** - Cell phones and other personal devices should be silenced and put away during class periods.

13. **Screen Time:** Media use and screen time are multidimensional; not all screen time is created equally. The global term “screen time” does not distinguish between different types of device usage: reading, writing, listening, collaborating, designing, creating, problem-solving, socializing, educational gaming, strategy gaming, and entertainment.
Screen time in class is monitored and limited by teachers and filtered for appropriate content. Students use devices in class for educational purposes. The District expectation is that screen time in the classroom should be limited to instructional relevant use only, and that instructional time should be focused on maximizing student learning including a mixture of face-to-face discussion and hands-on activities.
14. **No Expectations of Privacy:** No student shall have any expectation of privacy in any District-provided technology usage/storage including but not limited to computers, iPads, Chromebooks, Internet access, or wireless activity. The District’s system operators may access any electronic communication or files and may delete any inappropriate material found. All Internet activity is monitored and logged to ensure compliance with the Child Internet Protection Act (CIPA) and Children’s Online Privacy Protection Act (COPPA). In addition, discipline may be imposed for improper usage.
15. **No Warranties:** The District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided. It shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any student or his or her parent(s) or guardian(s) arising out of the student's use of its computer networks or the Internet.
The student or, if the student is a minor, the student's parent(s) or guardian(s) agree to cooperate with the school in the event of the school initiating an investigation of a student's use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the District's network.
16. **Application and Enforceability:** The terms and conditions set forth in this agreement shall be deemed to be incorporated in their entirety in the Network and Internet Acceptable Use Agreement executed by each system user.
BY EXECUTING THE APS NETWORK AND INTERNET RESPONSIBLE USE AGREEMENT AND THE APS TECHNOLOGY EXPECTATION AGREEMENT, THE SYSTEM USER AGREES TO ABIDE BY THE TERMS AND CONDITIONS CONTAINED IN THE ALTUS PUBLIC SCHOOLS ACCEPTABLE USE AGREEMENT. THE SYSTEM USER ACKNOWLEDGES THAT ANY VIOLATION OF THIS ACCEPTABLE USE AGREEMENT MAY RESULT IN ACCESS PRIVILEGES BEING REVOKED, DISCIPLINARY ACTION BEING TAKEN, INCLUDING, AS TO STUDENTS, DISCIPLINARY ACTION UNDER THE District's STUDENT DISCIPLINE POLICY AND, AS TO EMPLOYEES, ANY SUCH DISCIPLINE AS MAY BE ALLOWED BY LAW.

17. **Fees and Costs:** All iPads, Chromebooks, and accessories issued by Altus Public Schools that are stolen, lost, vandalized, and other malicious acts are subject to fees and costs associated with the replacement or repair of items, which become the responsibility of the student and/or the student’s guardians. The fees for replacement or damages are as follows:

iPad ($299) Chromebooks ($299)

iPad Charger ($15) Chromebook Charger ($30)

iPad Cable ($10)

iPad Case ($80)

Consequences for Violations: Consequences will be determined based upon the type of violation, and past history. Penalties for violations may include, but are not limited to: parent notification of the incident, loss of Internet and/or network access, and/or behavioral consequences. Certain violations for misuse of technology may lead to additional, more severe penalties and legal action, as applicable. If the District becomes aware that a user may have violated the law or board policy, an individual search of the user's files, Internet usage, or other electronic/digital media will be conducted. Seizure of the device may also be expected. The investigation and its scope will be reasonable and calculated to disclose the existence and nature of the alleged violation.

Zac Caffey
Director of Technology
Altus Public Schools
Phone: (580) 481-3098