أكاديمية الملك عبدالله
KING ABDULLAH ACADEMY

STUDENT BRING YOUR OWN DEVICE
INTERIM ACCEPTABLE USE TECHNOLOGY POLICY (AUTP)

King Abdullah Academy will now allow students the opportunity to bring their own personal mobile devices to school for educational purposes. A guest wireless network will be provided for the Internet. The guest wireless network is configured using best practices to filter known inappropriate websites. Access to the Internet via the guest wireless network, as well as use of any of the school's Information Technology, must be utilized solely for educational purposes. Students may use their devices to access and save information from the Internet, collaborate with other learners and utilize the productivity tools available to them. The policies in this agreement are pursuant and further to our Code of Student Commitment.

Cyber-bullying is bullying through the use of technology or any electronic communication, which shall include but not be limited to:

- harass, demean, humiliate, intimidate, embarrass or annoy others in their community.
- create a web page or blog in which the creator assumes the identity of another person
- knowingly impersonate another person as the author of posted content or messages.
- distribute by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more person.

Use only those computing and information technology resources for which you have authorization. Violations, include the following but are not limited to:

- use resources that you have not been specifically authorized to use
- access files, data or processes without authorization; or
- purposely look for or exploit security flaws to gain system or data access.

Use computing and information technology resources only for their intended purpose to conduct any activity considered illegal under federal and state law. Violations, include the following but are not limited to:

- send forged email
- misuse Social Media or other communications software that appears to allow students to hide their identity or to interfere with other systems or students
- use electronic resources for harassment, bullying or stalking other individuals
- send threats or "hoax messages"
- send chain letters

- intercept or monitor any guest wireless network communications not intended for you
- use computing or guest network resources for advertising or other commercial purposes to attempt to circumvent security mechanisms.
- create a web page or blog in which the creator assumes the identity of another person
- knowingly impersonate another person as the author of posted content or messages.
- distribute by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more person.

Protect the access and integrity of computing and information technology resources. Violations, include the following but are not limited to:

- release a virus or worm that damages or harms a system or guest wireless network
- prevent others from accessing an authorized service
- send email bombs that may cause problems and disrupt service for other students
- attempt to deliberately degrade performance or deny service
- corrupt or misuse information, or
- alter or destroy information without authorization.

Abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software. Violations, include the following but are not limited to:

- make more copies of licensed software/content than the license allows
- download, use or distribute pirated software/content
- operate or participate in pyramid schemes
- distribute or view pornography while on school property
- upload, download, distribute or possess child pornography.

Respect the privacy and personal rights of others. Violations, include the following but are not limited to:

- run guest wireless network sniffing/monitoring tools
- access or attempt to access another individual's password or data
- access or copy another student's electronic mail, data, programs or other files

أكاديمية الملك عبدالله
KING ABDULLAH ACADEMY

Recording, Video and Photography
Digital capturing device are permitted on campus, but should be used in a safe and appropriate manner within prescribed bandwidth limits. Capturing others in the KAA community on such devices (video, photo, audio or otherwise) is prohibited without the consent and intended use agreed upon by all parties. Google Glasses or any anonymous capturing devices are strictly prohibited from campus.

Website Usage and Social Networking
Users may access their own pictures or view other's pictures on photography sharing websites.

Users are not permitted to access from the KAA's guest wireless network any websites that involve rating or judging of another member of the KAA community. Users may not access material that is offensive, profane, or obscene including pornography and hate literature. Hate literature is anything written with the intention to degrade, intimidate, incite violence, or incite prejudicial action against an individual or a group based on race, ethnicity, nationality, gender, gender identity, age, religion, sexual orientation, disability, language, political views, socioeconomic class, occupation, or appearance (such as height, weight, and hair color).

KAA employees are not allowed to 'friend' current KAA students, or otherwise establish a direct social link with KAA students on social networking sites.

****

Right to Update
Since technology is continually evolving, KAA reserves the rights to change, update and edit its technology policies at any time in order to continually protect the safety and well being of our Users and community. To this end, KAA may add additional rules, restrictions and guidelines at any time.

أكاديمية الملك عبدالله
KING ABDULLAH ACADEMY

General Safety and Security Tips for the Use of Technology

Posting Online and Social Networking: Never post personal information about yourself online. Personal information includes your phone number, address, full name, siblings' names, and parents' names. When creating an account on a social networking website, make sure to set your privacy settings so only your friends can view your pictures and your profile. Avoid accepting a friend you do not already know. If possible, set up your account so that you are notified of any postings onto your wall or page. If possible, set up your account so that you have to approve all postings to your wall or page. If possible, set up your account to notify you when someone else has posted and tagged you in a picture. If you have a public profile, be careful about posting anything identifiable such as a sports team number or local park where you spend your free time.

Communications: Think before you send all forms of communication, including emails, IM's, and text messages. Once you send the data it is not retrievable, and those who receive it may make it public or send it along to others, despite your intentions.

Strangers: Do not feel bad about ignoring instant messages or emails from unknown people. Save all contacts from known or unknown people who are repeatedly contacting or harassing you. These saved messages will help authorities track, locate, and prosecute cyber-stalkers and cyber-bullies. If you have been speaking with a stranger online and make plans to meet the stranger in person, notify your parents or guardians first.

Passwords: Do not share your passwords with your friends. When creating a password, do not make it anything obvious such as your pet's name or favorite sports team. Also remember to include both letters and numbers in your password if possible.

Downloads and Attachments: Do not open or run files, or click on links in emails, on your computer from unknown or suspect senders and sources. Many viruses and other undesirable consequences can result from opening these items.

Stay Current: Do protect your own computer and devices by keeping antivirus and antispyware up to date. Keep your operating system and application software up to date. Turn off file sharing as an option on your computer.

أكاديمية الملك عبدالله
KING ABDULLAH ACADEMY

STUDENT BRING YOUR OWN DEVICE
INTERIM AUTP AGREEMENT

In accordance with the Seven Core Principles of King Abdullah Academy, I understand that I am a self-directed learner. I also understand that the use of the KAA guest wireless network is a privilege, not a right. Each Learning Community faculty will determine the appropriate use of all devices (laptops, tablets, cell phones, etc…), with the varying consequences being determined at each PLC leadership level. Inappropriate use may result in my suspension of those privileges in varying degrees and my suspension from school by the building administrator. I may be denied future computer privileges and I may be subject to further disciplinary, as well as legal actions for violation of copyright and/or licensing laws. I will be personally charged for any unauthorized cost incurred in their use of the KAA. I agree to report any knowledge of policy violations that I am aware of to the building's staff and/or administration.

For students: I have read the King Abdullah Academy Student Bring Your Own Device Interim Acceptable Use Technology and I agree to abide by its conditions.

_____

Please print student name (Required)

_____ _____

Student Signature **Date**

Updated November 15, 2016

أكاديمية الملك عبدالله
KING ABDULLAH ACADEMY

PARENT OR GUARDIAN
GUEST WIRELESS NETWORK AGREEMENT

As a condition of _____ (student) being permitted to use the King Abdullah Academy (KAA) guest wireless network, I have read the policy and this agreement. I understand that access to electronic information, which includes the Internet, is designed for educational purposes. Policies and procedures which require classroom teachers and library/media specialists to monitor and restrict access to inappropriate material are in place, but the KAA cannot monitor users at all times and thus cannot guarantee that students will not gain access to educationally-inappropriate material. Therefore, I will not hold KAA responsible for any inappropriate material acquired from this guest wireless network. In addition, I understand that KAA does not assume responsibility for the accuracy or reliability of information obtained through access to remote sites.

The use of online information retrieval and sharing is a privilege, not a right. Inappropriate use may result in a cancellation of this privilege and/or disciplinary action.

For Parents/Guardians: I have read the Student Bring Your Own Device Interim Acceptable Use Technology Policy as it relates to the Code of Student Commitment, and I agree to the terms of the AUTP as it relates to my child's usage of the guest wireless network provided by KAA. Please sign below and return to your child's school.

_____

Please print Parent/Guardian name (Required)

_____ _____

Parent/Guardian Signature **Date**

Updated November 15, 2016