



# THE KING'S ACADEMY

## TKA Device Acceptable Usage Policy 2020-2021

### Device Acceptable Usage

The term “computer device(s)” as stated herein, is defined as any school-owned device, or any personal device that is connected to TKA Bring Your Own Device (BYOD) network, such as a laptop, iPad, or any other mobile device. The term “loaner device” is defined as any device checked out by the IT Department to a student for the sole purpose of using on campus or at home for a short period of time while the student device is being fixed or replaced. The term “network services” refers to the school’s network and/or internet connections used to access school or internet-related information. That includes but is not limited to, wired and Wi-Fi connections.

### Acceptable Use

- a. Computer devices should only be used for educational purposes related to classroom work or school-related assignments throughout the school day.
- b. Students are only allowed one device on TKA BYOD network. iPads for junior high students and MacBook laptops for high school students are the only devices allowed on the student network.
- c. It is strongly recommended that students have no administrative rights on their devices and that the sole account with administrative privileges be the parent account.
- d. It is strongly recommended that students buy a hard cover for their devices to protect it from damage. Upon request, for iPads only, TKA may order the Logitech Rugged Combo iPad protective case and charge parents through their FACTS account.
- e. Parents agree that student personal devices will have antimalware software installed and that it will be constantly updated to keep the device secure. Additionally, the built-in firewall will be enabled at all times and the device will be kept up to date with the latest operating system and security updates. Any device that is suspected to have any form of malware will be taken off the network until it is remediated by the parents.
- f. Students must comply with the TKA IT policy published in this handbook, as long as they are on campus and connected to TKA network.

### Unacceptable Use

Unacceptable use of computer devices and network services includes, but is not limited to, the following:

- a. Students agree not to use computer devices for any purpose that is contrary to the mission, purpose, or belief of TKA, which is a biblically-based religious institution.
- b. Students may not use their devices for cheating and may not use text messaging platforms such as iMessage to communicate during school hours.

- c. Students are responsible for any activity that occurs when logged on to any school-owned computer devices such as lab computers or loaner devices. Students should never share their network or email passwords or allow another student to use their computer device. Doing so will result in the suspension of computer privileges for five school days for all students involved.
- d. Personal data should not be stored on any school-owned computer device. Personal data includes, but is not limited to, photos, documents, videos, etc. TKA is not responsible for the loss of any personal data saved on school computer devices.
- e. Students may not access, publish, post, forward or download inappropriate material; this includes, but is not limited to, pornographic, slanderous, defamatory, discriminatory, aggressive, bullying, harassing, alcohol-related, or drug-related material in any media format (such as all images and/or videos).
- f. Students may not use lab computers, personal or loaner devices for any illegal activity. Students may not attempt to evade TKA security systems and should report any such activity to the IT Director. TKA assumes no responsibility for any illegal activity made by the user while using computer devices or network services.
- g. Students may not download, copy, or publish any material that violates copyright or software licenses. TKA assumes no responsibility for copyright or licensing violations by users.
- h. Parents are aware that all activity will be monitored and filtered only while on campus and connected to the TKA network. Parental controls installed on student personal devices must be disabled during school hours so as not to interfere with school filtering systems and cause connectivity issues in the classroom.
- i. Students should not try to guess or bypass the BIOS password on any school-owned computer device.
- j. Students may not use computer devices for any personal reasons that are not in line with the school's educational program, classroom activity, or teacher assignments while connected to the TKA network. Examples of such activities include, but are not limited to, watching online series, movies, going on social media websites, playing online games, etc.
- k. Students are required to use the school's BYOD wireless network when on campus. Using personal hotspots or open wireless networks during school hours is not permitted. Parents agree that TKA is not responsible for any data charges that may incur due to using personal hotspots for any reason, be it school related or not.
- l. Tampering with user accounts in an attempt to lockout user accounts, or tampering with school-owned computer hardware is unacceptable.
- m. Access to online streaming websites is blocked for all students. YouTube access is allowed for students during school hours. Students should not attempt to bypass TKA's security to access those websites or any blocked website while connected to TKA network.
- n. Students must not use their personal devices to take photographs or video of others during school hours while connected to TKA network, unless specifically approved by a teacher.
- o. Students may not use their personal devices for hacking or to attempt access to private school networks; such activity will be detected and the device used to perform such activity will be collected and examined.

- p. Printing from personal devices to school printers is not allowed. Students who need to print must go to the library to use one of the computers assigned for printing.
- q. Students should not use any staff computer devices in any circumstance and for any reason.
- r. It is the students' responsibility to keep the devices fully charged before coming to school. Students should not expect to charge devices in the classroom.

### **Students Lost and Found Device**

- a. A student who leaves his/her device unattended will receive an electronic device misuse conduct report by the staff member who found the device; 5 demerits will be assigned for the first-time offense and then 10 demerits for consecutive offenses.
- b. Unattended devices found on campus will be turned in to the SAO.

### **Loaner Device**

- a. In the case that a student device is lost or broken and is in the process of being fixed, the TKA IT Department has a pool of loaner iPads and MacBooks. Those devices will be issued to students for a maximum of 5 days from the date it was requested, until they get their device fixed or replaced.
- b. Should the device repair extend beyond the 5 days, the students must bring the loaner device back to the IT department and request an extension. Extensions will be allowed only if we have enough loaners to accommodate other student needs.
- c. Loaner devices will have the same security controls as any school-owned computer device. Students will have to login using their TKA network account just like they do on their own device to get access to the Internet.
- d. Installing any software on loaner devices is strictly prohibited. If any student installs unauthorized software, it will be necessary for the IT Department to restore the computer to its original state. This process is time-consuming and will be billed to the parents at a rate of \$45 per hour.
- e. Damage to loaner devices will be treated the same way as it is for a school-owned device. Please refer to the section "Lost, stolen or damaged device policy" for more information. If a student damages the loaner device, they will not be issued another one and will have to wait until their device is repaired.

### **Lost, stolen or damaged device**

- a. It is the responsibility of the students and family to safeguard their personal computer devices.
- b. Device insurance can be purchased online for those whose homeowner's or renter's insurance does not offer coverage. TKA is not responsible for any damage or theft of personal devices.
- c. For any technical issues pertaining to computer device connectivity to the TKA network, students must ask their teacher to create a ticket by sending an email to [help.desk@tka.org](mailto:help.desk@tka.org), if they can't create the ticket themselves.
- d. The IT department will only provide technical support for connectivity issues to the TKA BYOD network. Neither IT members, nor any staff will help troubleshoot, repair, or fix any technical issues related to the personal computer device or any software installed on it.

- e. Parents agree that if the student's personal device is damaged, lost, or stolen, it will be their responsibility to repair or replace the device in a timely manner and not rely on the school-issued loaner devices.

**Student Withdrawal from TKA**

- a. Should a student withdraw from school, any loaner device issued to them must be returned in good working condition, without any damage. Parents agree that they will be responsible for any damage that may occur to the loaner device while in their possession.

If you need to contact the TKA IT Department for any assistance, please email [help.desk@tka.org](mailto:help.desk@tka.org).

## HANDBOOK

### **INFORMATION TECHNOLOGY POLICY AND GUIDELINES**

This section provides specific guidelines for students and parents in using TKA's computing services including, but not limited to, computer hardware, software, email, and internet access, collectively referred to as Information Technology (IT). IT services at TKA are provided to enhance education at the school.

#### **General Policy**

- The school will support a process to monitor internal compliance with the school's internet operations, specifically in relation to the internet access policy. Monitoring will include the right to review any downloaded information from the internet, electronic software, product, and/or service to ensure it is virus-free and in compliance with relevant copyright laws and regulations. All network activity is continuously monitored and filtered while connected to the TKA network.
- Misuse of internet access privileges may ultimately expose the school to civil and criminal penalties and/or liability. Failure to follow these guidelines may result in the elimination of that individual's internet access privileges and/or other disciplinary actions such as verbal warnings (censure) and written warnings, depending on the significance of the abuse of privileges.
- Should the question arise of whether an action or activity via the internet would violate school policies and regulations, guidance or direction should be requested from the IT Department by emailing [help.desk@tka.org](mailto:help.desk@tka.org) or contacting the IT Director, Magdy Abadir, at [mabadir@tka.org](mailto:mabadir@tka.org).

#### **Students Account**

- Student Account Information sheets for new students include all necessary students account login information and will be distributed and can be picked up from the IT Department during textbook distribution week.
- Each student will be given one email address during their enrollment at TKA. There will be no additional email addresses or email aliases created for students for any reason.
- TKA students withdrawing from TKA will have all of their accounts disabled on their last day of school.
- Graduating seniors will have their TKA accounts disabled on August 1<sup>st</sup> by 5:00 p.m. Seniors should use a personal email to communicate with colleges prior to their TKA account termination. An email will be sent out from the IT Department to senior students during the first week of May with information on how to download their Google data to their computers.
- Student accounts that have been disabled will not be reinstated for any reason. Students must download all of their data and update their contacts with their personal email prior to their accounts being disabled. Accounts will not be re-enabled for any reason after August 1.

#### **Internet/Network Access**

TKA has provided students with many technical tools and learning aids that will better their learning experience. It is the responsibility of all TKA students to take proper care of these tools and aids as good stewards of the things that God has provided. These policies and procedures reflect that responsibility and help the IT Department to serve the TKA community better.

- All school communication services and systems, hardware, and software are considered school property; accordingly, the IT Department may review and monitor the use of the school property as well as the data and/or communications sent, received, and/or stored.
- Parents and students are aware that connecting their personal computer devices to TKA BYOD network is done at their own risk. It is the responsibility of the student to maintain the upkeep and security of their devices and their personal accounts.
- All data stored on Google G Suite or any computer device owned by TKA that is on or off campus is solely owned by TKA.
- Using network access to break or attempt to break into systems inside or outside of the school network in order to gain access to resources for any reason is strictly prohibited.
- The IT Department reserves the right to block access to certain internet websites and/or other services that are not in line with the school's code of ethics, beliefs, or business operations through the use of a content filter. Any attempt to bypass the filter by installing VPN software and/or browser extensions will be logged, and disciplinary actions will be issued accordingly.
- Students may not share with other students any websites or any other resources that will give them access to websites blocked by TKA.
- Attempting to gain access to files or communications on other users' computers for satisfying idle curiosity with no substantial purpose, unauthorized access to data or attempting to breach any security measures on any electronic communication system, or attempting to intercept any electronic communication transmissions without written authorization is forbidden.
- The use of Peer to Peer (P2P) file-sharing programs such as BitComet, BitTorrent, and the like are strictly forbidden on any computer connected to the school network. This includes personal laptops, school-issued loaner devices, and any device connected to the school's wireless network.
- Personal devices will not be allowed on TKA's restricted wireless network; however, an open Wi-Fi network will be available to TKA guests. No one should install a rogue access point or network device and connect it to the TKA network to gain access to a local network or the internet. Network cables from a computer or network device may not be removed and connected to a personal device. Actions such as these will be dealt with as an attempt to bypass TKA security. Violators will be tracked, and disciplinary actions will be taken by administration.

### **Software and Personal Device Content**

- Teachers may require the installation of apps/software that are used for classroom activities. Parents may inform teachers that their student may not do so without getting prior approval from the parent.
- Any device connecting to the TKA BYOD network should not contain any software or apps that may be used to access illegal, copyrighted content, or inappropriate file sharing sites.
- If any student installs unauthorized software on their personal device, which includes, but is not limited to, VPN software, proxy extensions, torrents, network games, etc., it is their responsibility to make sure not to use this software while connected to the TKA BYOD network.