# Technology Device Procedures and Expectations

## Knox County Schools

Updated Spring 2016

## DISTRICT POLICIES AND PROCEDURES

Board of Education policies and Knox County Schools procedures that are relevant to the use of technology devices include but are not limited to the following:

IFABC- Internet Safety Policy
JCADA- Harassment, Intimidation and Bullying or Cyber-bullying
MC-107- Access to Electronic Media Form
MC-108- Guidelines for Acceptable Use of Electronic Media Form

All policies are located www.knoxschools.org (Board of Education tab).

## EXPECTATIONS

**RECEIVING a Technology Device:**

- A system-wide process for training and deployment will occur for each school's student deployment.
- Training/deployment dates will be staggered by school site. There will be multiple sessions for each school to accommodate students, parents/guardians and school staff.
- Parents/guardians are required to attend the training for all students who receive a technology device. Students and parents who are "returning" to a school will attend a "shorter" version of the training.
- The session will consist of completion of paperwork and training sessions for students and parents/guardians.
- Parent/guardian and student must sign and return the Knox County Schools Technology Device Agreement before the device can be issued to the student.
- All previous fines must be paid in order to receive the technology device or the student will remain a day user until the fines are reconciled.
- Students will use technology devices in a manner consistent with All Board of Education policies and district procedures and school rules.

**Students will not receive their technology devices until their parents/guardians have cleared any technology fines, attended a training session, and signed the appropriate paperwork.**

**RETURNING a Technology Device:**

- The individual's school technology device and accessories (technology device and charger, as well as any additional protective covering provided by the school) must be returned to the school at the end of each year.
- Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment for any other reason must return their school technology device on the date of termination.
- If a student fails to return the technology device at the end of the school year or upon termination of enrollment, that student/parent/guardian will be subject to a **student fine** for the replacement cost of the device per the KCS scale (KCS Board Policy- JS- Student Fees and Fines). The technology devices are property of Knox County Schools.
- The student will be responsible for any damage to the technology device, charger, or protective covering. The student will be charged for any needed repairs, not to exceed the replacement cost of the technology device.

Throughout the remainder of this document, the term **Technology Device** includes the device, charger, warranty, and any protective covering if provided.

**Technology Device Use**

• The care of the district technology device is the student's responsibility. Students should not lend their technology device to another person. Each technology device is assigned to an individual student and the responsibility for the care of the technology device rests solely with that student.

• Students should never leave the technology device unattended. When not in a student's possession, the technology device should be in a secure, locked environment (For example, students are strongly encouraged to have locks on their school lockers).

• Students need to charge their technology device each night at home so that it is fully charged when they arrive to school each day.

•Failure to bring the district issued technology device (no personal home device) or other class materials does not release a student from his/her responsibility for class work. If a student repeatedly fails to bring materials to class, including the technology device, progressive discipline procedures will be followed.

•**The technology device is the property of the Knox County Schools and may be collected and inspected at any time. Students have no right to privacy for any material on a district technology device**.

•Each technology device has a unique serial number and asset tag. Students should not modify or remove the tag. *Students should not write on, draw on, or add stickers or labels directly to the technology device*. No form of tampering will be permitted.

• **It is the student's responsibility to back up projects and content.** Students may want to purchase a flash drive for this task or plan to store their materials in "the cloud."

• Students with MacBooks or iPads may add their iTunes account to their device. This information may be inspected on the district technology device and inappropriate, graphic, or offensive material may be removed and disciplinary action taken in accordance with the school handbook and aligned to district policies.

• If a student's technology device is not working or is damaged, students should report the problem immediately to the help desk.

•If a student's technology device is lost or stolen at school, the student should report the loss immediately to the school administration. If a student's technology device is lost or stolen outside of school, parents/guardians should report the loss immediately to the local police and obtain a police report (see page 9 for protocol).

• Students are responsible for using the technology device according to school and district policies and procedures.

# TECHNOLOGY DEVICE GUIDELINES AND EXPECTATIONS

**Care & Maintenance**

- Devices should NEVER be picked up by the lid. Students should close the technology device before it is picked up.
- Students will use the school issued protective covering if provided.
- When carrying the device to and from school campus, it is expected that the device will be placed in a backpack, bag, or other carrying case.
- It is recommended that if students use a backpack, then the technology device should always be placed in the backpack with the port-side facing up to keep pencil lead and other debris from jamming the ports.
- Technology devices should be kept at room temperature and should NOT be exposed to extremes of hot or cold. Students should **NOT LEAVE their technology device IN AN AUTOMOBILE. Students should not leave their technology device outside.**
- Liquids and food should not be used/consumed in the vicinity of the technology device.
- Cleaners, sprays, alcohol, ammonia or abrasives should not be on the technology device. Devices should be cleaned with a soft, lint-free cloth.
- The device should remain in the protective cover when not in use. Device should not be in a place where someone could accidentally sit or step on it.

**Technology Device Parent/Guardian Guide**
**Additional resources can be found at www.commonsensemedia.org**

- Monitor your child's home use of the Internet with the technology device.
- Provide a place in an open area of your home, such as the kitchen or family room, where the technology device will be used.
- Use the Internet with your child to help develop safe Internet habits.
- Frequently ask to see your child's technology device and ask how it is being used.
- Review with your child the programs installed on the technology device and ask them what each program does.
- Do not hesitate to contact your school if you have any questions or concerns about the technology device.

**Maximize Battery Life**

Students should use the technology device in a way that maximizes its battery life.

- **Brightness:** Students should dim the screen to the lowest comfortable level to achieve maximum battery life. For instance, when watching a video in a dark room, you may not need full brightness.
- **Wireless:** Wireless connections consume power, even if you are not using its features to connect to a network. You can turn it off in the control panel to save power.
- **Bluetooth Wireless:** Likewise, you can turn off Bluetooth to maximize your battery life, as it also consumes power when not in use.
- **Applications and peripherals:** Disconnect peripherals and quit applications not in use. Eject CDs and/or DVDs if not currently accessing them.

# REPAIR AND REPLACEMENT GUIDELINES

The following is designed to be a guide and reference for dealing with issues related to student technology device damage with the understanding that the goal is for every student to have an operational device. Typically issues will arise over one of the following: Theft, Non-preventable Damage, Preventable Damage/Negligence, and Willful Damage/Recklessness.

*During the time of a review, the student will become a "day user" where they will check out a machine from the help desk each morning and return it before they leave school each day.*

***Theft***

• Administrator will meet with student and parent/guardian to investigate the theft.
• A police report is required to document a theft.
• After a police report is submitted, the student will be a day user during the time of the investigation. Upon finalizing the report, a student should be issued a new device.

***Non-preventable Damage*** (these are rare, but examples might include, but are not limited to: auto accident, house fire, etc.)

• Administrator will meet with student to investigate the incident and discuss with parent/guardian as necessary.
• Upon determination of a verifiable accident, the student will be issued another device.

***Preventable Damage/Negligence or Willful Damage/Recklessness***

• The parent/guardian and student have accepted responsibility for the technology device and therefore are liable for the cost of the repair or device (a cost scale available with KCS).
• Administrator will meet with student to investigate the incident and discuss with parent/guardian as necessary.
• Student will become a "day user" until the cost of the repair is received.
• The cost of repair will be to the student who caused harm.

The cost of repairs will be assessed for each reported incident. Multiple offenses should be handled appropriately and in consultation with the district office if necessary. Cost estimates are on the following page, please reference for the appropriate device.

| 13” MacBook Pro and 11” MacBook Air Replacement Maximum Cost by Purchase Year | | | | |
|---|---|---|---|---|
| | **Year 1** | **Year 2** | **Year 3** | **Year 4** |
| Standard Schedule 80/60/40/20 | Up to $800 | Up to $600 | Up to $400 | Up to $200 |
| Free/Reduced Schedule 40/30/20/10 | Up to $400 | Up to $300 | Up to $200 | Up to $100 |

| **Repair/Replacement** | **You Pay** |
|---|---|
| Display | Up to $260 |
| Keyboard | Up to $130 |
| Power Adapter/Extension Cord | Up to $50 |
| Tier IV repairs (Liquid spill, logic board) | Up to $500 |

The cost of repair/replacements will be as listed above or the maximum cost to replace the device (see page 11 for repair process and timeline).

| iPad Replacement Cost | |
|---|---|
| **Repair/Replacement** | **You Pay** |
| Replacement of iPad | Up to $500 |
| Display | Up to $180 |
| Headphone Jack or Charging Port | Up to $70 |
| Charger | Up to $40 |
| Case | Up to $20 |

| iPad Air 2 with 4G Replacement Cost | |
|---|---|
| **Repair/Replacement** | **You Pay** |
| Replacement of iPad | Up to $610 |
| Display | Up to $300 |
| Headphone Jack or Charging Port | Up to $80 |
| Charger | Up to $40 |
| Case | Up to $25 |

| Dell 11” Chromebook Replacement Cost | |
|---|---|
| **Repair/Replacement** | **You Pay** |
| Replacement of Device | Up to $250 |
| Display | Up to $135 |
| Headphone Jack or Charging Port | Up to $70 |
| Charger | Up to $25 |
| Top Case | Up to $70 |

**Additional Responsible Use Guidelines**

**A. GUIDELINES FOR USE OF TECHNOLOGICAL RESOURCES**

- Users may not intentionally or negligently damage devices, technology device systems, electronic devices, software, system networks or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit viruses or self-replicating messages or deliberately try to degrade or disrupt system performance.
- Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network.
- Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the network to gain or attempt to gain unauthorized or unlawful access to other computers or devices, computer systems or accounts.
- Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual, the teacher or other school official.
- Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.
- Users shall not use passwords or user IDs for any data system (e.g., Active Directory, Canvas, etc.), for an unauthorized or improper purpose.
- If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
- Views expressed on the Internet or other technological resources as representing the view of the school district or part of the school district may only occur with prior approval by the superintendent or designee.
- Without permission, users may not connect any personal technologies such as technology devices and workstations, wireless access points and routers, etc. to a district owned and maintained local, wide or metro area network.
- Those who use district owned technology devices will have access to the Internet while at the school. It is not necessary to have Internet access at home. If a family chooses to have Internet service at home, they are responsible for both the cost and configuration of this service.

**B. RESTRICTED MATERIAL ON THE INTERNET**

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. It is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless school district personnel will endeavor to take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose.

If content, which might be considered sensitive, is used during a course, teacher will review the materials according to KCS Board Policy- IFAB- Selection of Instructional Materials (Other than Textbooks).

KCS Board Policy- IFAB- Selecting Instructional Materials Other than Textbooks

*Any instructional materials that include content which might be considered sensitive by parents/guardians or students (for example, materials that might contain coarse language, graphic violence, explicit sexual content, illegal use of drugs or alcohol, acutely illicit activity, malicious denigration of religious beliefs, and/or extremist inducements) must be assessed and approved at the school level using the Instructional Materials Assessment (IMA) process prior to being assigned. For instructional materials that include potentially sensitive content, the IMA documentation must be reviewed and approved by the school principal prior to their assignment. If such instructional materials are assessed and reviewed at the school level and it is determined that their literary and/or educational value greatly outweighs the concerns over the sensitive material, then the materials may be utilized, but only if clear, timely, and detailed notification is made to students and parent/guardians about the sensitive content, and alternative materials are offered and communicated at the time of the assignment.*

**C. PARENT/GUARDIAN CONSENT**

We recognize that parents/guardians of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent/guardian must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent/guardian and student must consent to the student's independent access to the Internet (MC-107 to withhold permission) and to monitoring of the student's communication by school personnel.

**D. PRIVACY**

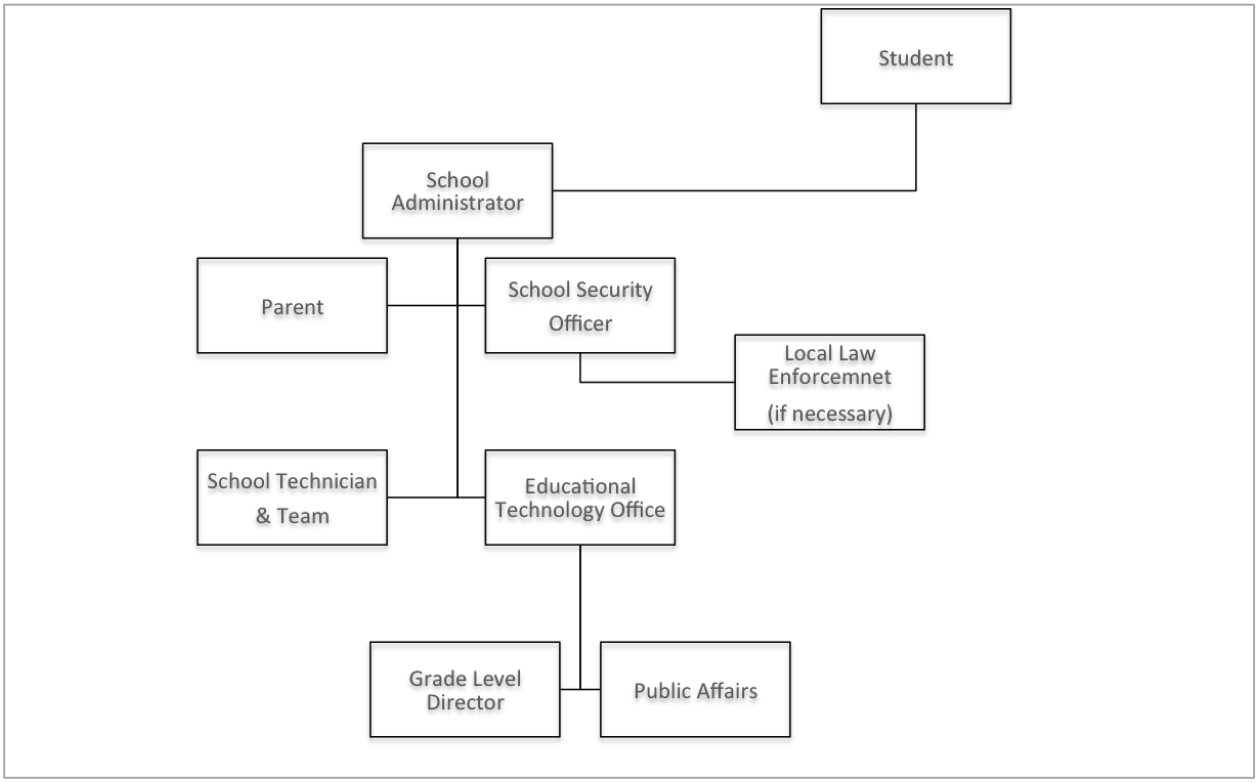
No right of privacy exists in the use of technological resources. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual devices will be private. School district administrators or individuals designated by the superintendent may review files, observe screen activity, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel will endeavor to monitor on-line activities of individuals who access the Internet via a school-owned device. Under certain circumstances, the school may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit.

**E. SECURITY/CARE OF PROPERTY**

Security on any technology device system is a high priority, especially when the system involves many users. Users are responsible for reporting information security violations to appropriate personnel. Users should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system device on the network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access. Users of school district technology resources are expected to respect school district property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for devices while under their control. The school district is responsible for any routine maintenance or standard repairs to school system technology devices.

# Protocol for Stolen Student Devices while On Campus

In the diagram below, the student's only obligation in the event of a theft is to report it directly to a school administrator. The remaining steps in the process will occur in collaboration with the parent, school administration, technical team, and school security.




**<u>If the device is stolen Off Campus</u>**

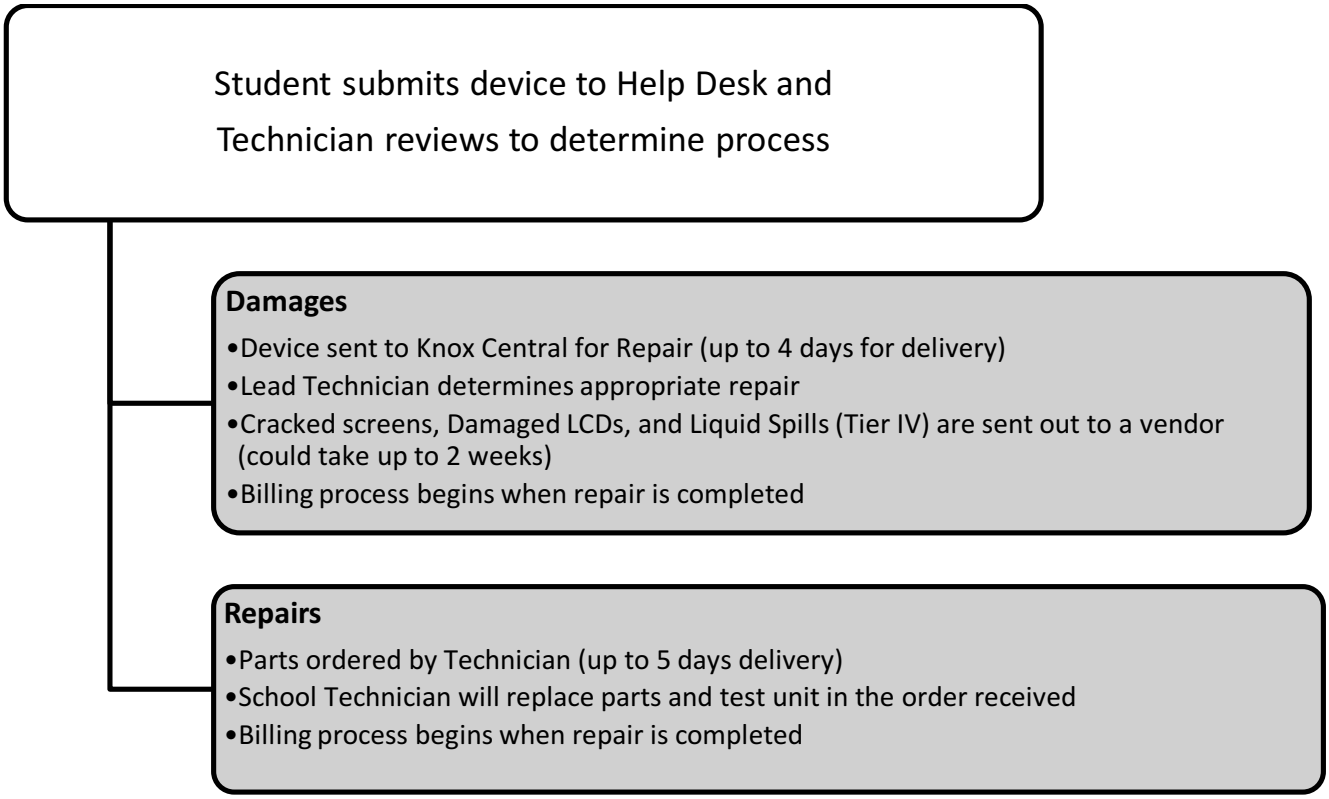
The student and parent are responsible for contacting law enforcement as soon as possible, getting a police report, then following the on campus protocol on the next business day.

**<u>If the device is found</u>**

The device should be returned to the Administration/School Security Officer to determine if it should be

1) "Wiped" and Re-imaged to return to the student OR
2) The device should be handled as evidence and given to law enforcement.

## Knox County Schools – Process for Device Repairs




The student will be issued a “loaner” device to be used while repairs are being made.