# Technology Responsible Use
## (Responsible Use Policy for Staff and Students in Deployment Schools)

Shelby County Public Schools and its Board of Education (hereafter referred to as "the District") provides its student, staff and community reasonable access to a variety of "district technological resources" (including, but not limited to, access to the Internet and laptop computers). These resources provide opportunities to enhance learning, improve communication, and connect users to both our local and global community. The access to these resources is permitted when exercised in an appropriate and responsible manner as required by this policy and related procedures, which applies to all parties who use District technology.

The District intends that students and employees benefit from these resources while remaining within the bounds of safe, legal and responsible use. Accordingly, the District establishes this policy to govern student and employee use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

## A. REQUIRED EXPECTATIONS FOR USE OF DISTRICT TECHNOLOGY (GENERAL)

School district technological resources may be used by students, staff and others only with authorization by the District. The use of district technological resources is a privilege, not a right. Individual users of district technological resources are responsible for all behavior and communications when using those resources. Responsible use of school district technological resources is use that is ethical, academically honest, supportive of student learning, and respectful. General student and employee behavior standards, including those prescribed in applicable board policies, school handbooks and other regulations and school rules, apply to the use of the Internet and other school technological resources.

Additional rules are outlined below for Employees (Section B) and Students (Section C). These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive. Prior to using the Internet and/or access to school technology, all students must receive initial training about appropriate online behavior (initially provided at device deployment). **(SC Policies 03.1321, 03.2321, and 09.4261)**

Prohibited use includes using digital resources to establish third-party email accounts not administered by the District, as well as accessing sexually explicit materials. District materials shall not be used for any purpose prohibited by law, including those relating to copyrights and trademarks, confidential information, and public records.

Individuals shall reimburse the District for repair or replacement of District property lost, stolen, or damaged while under their care. Individuals are responsible for turning in district technology such as laptops to their

school or the District's central office in a timely manner when they are no longer students or employees of the district. This technology should be in at least as good condition as when it was taken possession by the user, accommodating for normal wear and tear over time. Students and staff members who deface a District web site or social media account, or otherwise make unauthorized changes, shall be subject to disciplinary action, up to and including termination (employees) and expulsion (students) as appropriate.

Before using school district technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements. In the case of students, their parent/guardian must also co-sign this statement. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. For students with take-home district devices, a violation may result in becoming "day-users" who must check out their device every morning and return it every day at the end of school. Willful misuse may result in in disciplinary action and/or criminal prosecution under applicable state and federal law, up to and including termination (employees) and expulsion (students) for violating this policy and responsible use rules and regulations established by the school or District.

**B. RESPONSIBLE USE OF TECHNOLOGY BY EMPLOYEES**

1. Employees are responsible for the security of their individual passwords.
2. Employees are encouraged to use electronic mail and other District technology resources to promote student learning and communication with the home and education-related entities. If these resources are used, they shall be used for purposes directly related to work activities. All work-related email should not be deleted for a period of two (2) years.
3. Technology-based materials, activities and communication tools shall be appropriate for and within the range of knowledge, understanding, age and maturity of students with whom they are used. To ensure this, teachers shall make reasonable efforts to supervise students' use of district technology (including laptops and access to the Internet) during instructional time.
4. District employees and activity sponsors may set up blogs, websites, and other social networking accounts using District resources and following District guidelines to promote communication and learning with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction. However, district employees shall not create or use personal existing social networking sites to which they invite students to be friends or otherwise "follow" them.
5. In order for District employees and activity sponsors to utilize a social networking site for instructional, administrative or other work-related communication/learning purposes, they shall comply with the following:
    a. Staff members will set up the site following any District guidelines developed by this policy and the supervisor.
    b. Guidelines may specify whether access to the site must be given to school / District technology staff.
    c. The sponsoring staff member is responsible for the following:
        i. Monitoring and managing the site to promote safe and acceptable use; and

ii. Observing confidentiality restrictions concerning release of student information under state and federal law. This includes the release of video, still pictures, or audio of a student to the general public without permission to capture being granted by a parent/guardian. For more information about employee limitations on capturing video or audio or taking pictures. **(SC Policy 03.23214)**

6. All employees shall be subject to disciplinary action if their conduct relating to use of technology or online resources violates this policy or other applicable policy, statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety and emotional well-being of students and confidentiality of student information. Conduct in violation of this Code, including but not limited to, such conduct relating to the use of technology or online resources, must be reported to Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

## C. RESPONSIBLE USE OF TECHNOLOGY BY STUDENTS

1. Students will initiate digital citizenship requirements before given access to district technological resources. This begins with the orientation about digital citizenship at the laptop deployment. Additional training will be conducted during the day as needed.
2. School district technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. This regulation of use includes the use of a district device in all environments, including but not limited to school, home, or extracurricular functions.
3. Students should not attempt any installation of programs or maintenance without the permission of the District IT department or its designees.
4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors. All uses must comply with policy on harassment when using district technology. **(SC Policies 03.162, 03.262, 09.42811)**
5. The use of anonymous proxies to circumvent content filtering is prohibited.
6. Students may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.
7. Under no circumstance may software purchased by the school district be copied for personal use.
8. Users of technological resources may not send electronic communications fraudulently (i.e. by misrepresenting the identity of the sender).
9. Students must respect the privacy of other students and staff members. When using emails, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information, or information that is private and confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students. For further information regarding what constitutes personal identifying

information. **(SC Policy 09.1)** Users also may not forward or post personal communications without the author's prior consent.

10. Students should not capture audio, video or still pictures of other students and/or staff members, nor share such media in any way, without consent of the students and/or staff members and the approval of the appropriate Principal or designee. (Note that exceptions to this may include settings where students and staff cannot be personally identified beyond the context of a sports performance or public event.)
11. Students may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to district technological resources. Students may not knowingly or deliberately try to degrade or disrupt system performance, including streaming audio or video for non-instructional purposes.
12. Students may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the express permission of the district IT department or its designee.
13. Students are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.
14. Students are prohibited from using another individual's ID or password for any technological resource; they also are not allowed to read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.
15. If a student encounters a security or other problematic issue on a technological resource, he or she must immediately notify a teacher, administrator, or IT department technician.
16. Personal devices will not be supported by District staff. The District is not responsible for the content accessed by users who connect to the Internet via their personal mobile device and non-school network (e.g. cellular services).
17. Students are responsible for backing up data regularly. If using a cloud-based system to save work, students must be aware when or if the wi-fi is not functioning.
18. Students who use district owned and maintained technologies (such as laptops) to access the Internet at home are responsible for both the cost and configuration of such use. For more on home use of district technology, see Section D below.
19. Students who are issued "take home" district-owned technology (such as laptops) must also follow these specific guidelines: .
    a. Charge the devices nightly at home before returning to school, so they are fully charged (100% battery) for the beginning of the next school day.
    b. Bring the device every day to school for instructional use.
    c. Have the device always available to present to District staff. If a student is unable to present their device for three (3) consecutive school days, the device will be considered lost and appropriate action will be taken, including but not limited to compensation for the cost of the device.
    d. Keep the device secure and damage free.
    e. Use the provided protective case at all times.
    f. Do not loan out the device, charger, case or cords.
    g. Do not deface the device itself with drawings, stickers or other permanent adornment.

h. Do not leave the device in your vehicle.
i. Do not leave the device unattended.
j. Do not eat or drink while using the device or have food or drinks in close proximity to the laptop.
k. Do not allow pets near the device.
l. Do not place the device on the floor or on a sitting area such as a chair or a couch.
m. Do not leave the device near table or desk edges.
n. Do not stack objects on top of the device. If there are any ventilation holes on the device, do not block or obstruct them while the device is powered on.
o. Do not leave the device outside.
p. Do not use the device near water such as a pool or bathtub.
q. Do not check the device as luggage at the airport.
r. Make sure to back up files regularly (via a cloud-based system like Google Drive or via a storage device like a thumb drive) as crashes may occur and the device may need replacing or re-imaging.
s. Devices must be turned in at the end of the school year for maintenance and re-imaging (see R above). Take good physical care of your device, because when devices are deployed at the beginning of your school year, you will get the exact same one back.
t. Failure to follow these guidelines may result in becoming a "day-user" who must check out their device every morning and return it every day at the end of school.

**D. PARENTAL CONSENT**

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. The District recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless, the District shall take reasonable precautions to prevent students from accessing material and information that does not serve a legitimate educational purpose or is otherwise harmful to minors. These precautions include (but are not limited to) filtering software, maintaining a secure usages log, and educator monitoring and mindfulness of student Internet access in school. **(SC Policy 09.4261)** The District is not responsible for the content accessed by users who connect to the Internet via their personal mobile device and non-school network (e.g., cellular services).

The District recognizes 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 and/or use district technological resources, the parents/guardians must sign their student's Responsible Use Policy form as consent to the following:

1. Parents/guardians must be aware that a student could obtain access to inappropriate material while engaged in independent use of the Internet.
2. Students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals.

3. The District is not responsible for filtering the Internet access of students at home. If parents/guardians feel uncomfortable with allowing district devices (such as laptops) into their home, they can request for the student to be only a “day-user” of the device, who will check out the device every morning and turn it in every afternoon before leaving school.

**E. 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 (such as the district’s Google Apps for Education cloud-based Drive) or hard drives of individual computers will be private. School district administrators or individuals designated by the superintendent may review files, 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 may monitor online activities of individuals who access the Internet via a school-owned computer.

Under certain circumstances, the District 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 against the board, as a response to a public records request, or as evidence of illegal activity in a criminal investigation.

**F. DISCLAIMER**

The District makes no warranties of any kind, whether express or implied, for the service it is providing. The District will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the school district’s or the user’s negligence, errors or omissions. Use of any information obtained via the Internet is at the user’s own risk. The District specifically disclaims any responsibility for the accuracy or the quality of information obtained through its Internet services.

**References:**
03.1321
03.2321
09.4261
03.23214
03.162
03.26
09.42811
09.14.