Spartanburg School District Four

Access to Digital Devices and Internet for Learning

2021-2022

Overview

Spartanburg School District Four (SD4) views the use of electronic resources as an avenue to enrich curriculum and promote a collaborative learning environment for all students. Ethical and responsible conduct is required while engaging in electronic resource activities. With this privilege, comes responsibilities for the student and parent/guardian.

When signing the Student/Parent Technology Device Agreement, you are acknowledging that you understand and accept the information in the document.

SD4 students and parents/guardians must understand that:

- Students and families must follow all guidelines set forth in this document and by SD4 staff.

- The term "equipment" or "technology" refers to devices, batteries and power cords, chargers, and cases. Each piece of equipment is issued as an educational resource. The term "device" includes iPads, Laptops, Chromebooks, and district issued hotspots.

- **Ownership-** All devices are on loan to students and remain the property of SD4. SD4 retains sole right of possession and ownership and grants permission to the student to use the device according to the rules and guidelines set forth in this document and outlined by individual schools. Students will want to take care of the devices provided to them as it will be used by the student from one school year to the next. Failure to follow the terms and policies will result in disciplinary action, including but not limited to, confiscation of any and all devices and accessories lent to the student and revocation of student access to SD4 technology as well as any other disciplinary action deemed appropriate by SD4 or individual school policy. SD4 may remove a user's access to the network without notice at any time if the user is engaged in unauthorized activity.

- **Device Security and Monitoring-** SD4 reserves the right to monitor and log student use of district devices and network and to examine student files and material as necessary. SD4 staff retains the right to collect and/or inspect the device at any time, including via electronic remote access. All files stored on SD4 equipment, the network, or cloud services are property of the district and may be subject to review and monitoring. There is no reasonable expectation of privacy while using SD4 computers, networks, or technology.
    - **Balanced Approach-** Two primary forms of security exist: device security and internet filtering. Each device has a security program installed. SD4 strives to create a balance between usability of the equipment and appropriate security.
    - **Device Security-** Security is in place on the device to prevent certain activities. These include downloading or installing software on devices, removing software, changing systems, etc.
    - **Internet Filtering-**SD4 maintains an internet filtering software package. This program automatically filters all student access to the internet through the SD4 device, regardless of school/home use. District issued hotspots include a filtering software to ensure CIPA compliance for any device that connects to the internet.

- **Policy-** All users of the SD4 network and equipment must comply at all times with SD4 Board Policy IJNB as well as school, district, local, state, and federal laws.
  http://www.spartanburg4.org/departments/district_administration/policy_manual

- **Use-** Use of the devices and internet must support education. Internet access is filtered for CIPA compliance on devices and district-owned mobile hotspot. Each hotspot device comes with a monthly plan of high-speed data that should be used for the sole purpose of promoting educational learning. **All rules and guidelines are in effect for all SD4 devices whether on or off school campus.**

Student Responsibilities:

- Bring the District-Owned Device to School
    - Each student must bring his/her district-owned device to the school every day that classes are in session.
    - Students hold and maintain responsibility to ensure their device is charged prior to each school day.
    - The student's district-owned device and equipment are strictly for educational purposes. Using the district-owned device for recreational use ("gaming") during class time is strictly prohibited. Students are expected to fully participate in all classroom activities as directed by the teacher. In addition to the rules and guidelines set forth in this handbook, students must abide by all rules and guidelines set forth by their teacher/school.
- Students are expected to report loss or theft of technology devices immediately to their school as well as report any damage to their device or hotspot. This means no later than the next school day. In the event equipment is stolen, a police report must be filed and a copy of the report must be provided to the school by the student or parent in a timely manner. If there is not clear evidence of theft, or the equipment has been lost due to student negligence the student/parent may be responsible for the cost of replacing the item(s) at current cost.
- Students are expected to notify their school immediately if they encounter information, images, or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
- Students may only log in under their assigned username. Students may not share their password with other students.
- Students may not loan their district-issued device or hotspot for any reason.
- Students may not use a proxy to circumvent the firewall under any circumstances. **This is strictly prohibited and could result in disciplinary actions.**

Parent/Guardian Responsibilities:

- **Sign the Technology and District Owned Device Agreement and Complete Payment for the Technology Protection Plan.** In order for students to be issued a device, a student and their parent/guardian must sign the Student/Parent Technology Devices Agreement and pay the yearly $30 Technology Protection Plan fee. This is a nonrefundable (yearly) fee that covers the following accidental damage:
    - Cracked Screen
    - Damaged Casing
    - Broken Keys/Keyboards
    - Damaged Ports

For the Technology Protection Plan to remain valid, protective casing must stay on the device at all times. Please note loaner devices <u>may not</u> be available while the student district-issued devices is being repaired.

<u>Damage not covered under Technology Protection Plan are as follows</u>:

- **Liquid Damage (including but not limited to): spilled drinks, device submersion, natural damage (left in the rain even though in the student's book bag), etc.**
- **Total Loss of the Device*:** The device is damaged beyond repair and no part of the device is salvageable. (Examples of Total Loss: Run over by a car, submerged in the bathtub, disassembling any part of the device.) **Total Loss of Device will be examined by the insurance provider on a case-by case incidence.**
- The parent/guardian must agree to monitor student use at home and away from school. The best way to keep students safe and on-task is to have a parent/guardian present and involved.
- While internet access on devices and through district supported hotspots are already filtered for CIPA compliance at school and away from school, develop a set of rules/expectations for device use at home.
- It is recommended that device use only be allowed in common rooms of the home (e.g. living room or kitchen) so supervision of student use is always monitored.

***Should a device be deemed a total loss by the insurance company, the student will be charged the total replacement cost.**

- **Chromebook- $200**
- **iPad- $250**
- **Hotspot- $50**

**** Power adapters/cords are not included in the yearly insurance plan and $20 will be billed for damaged or lost charging units.**

Device Rules and Guidelines

The rules and regulations are provided here so that students and parents/guardians understand the responsibilities when they accept use of a district-owned device. In general, this requires legal and ethical utilization of all technology resources. Violations of these rules and guidelines could result in disciplinary action.

General Guidelines: Use of technology resources on and off campus at all times must:

- Support learning
- Follow local, start, and federal laws
- Be appropriate

Security Reminders:

- Do not share logins or passwords
  - (Exception: Students are asked to share passwords with parents/guardians)
- Do not develop programs to harass others, hack, bring in viruses, or change others' files
- Follow internet safety guidelines

Asset Tag: An asset tag is a barcode sticker placed on the device for inventory and monitoring purposes. All district-owned devices will be labeled with an inventory and asset tag. Tags may not be modified or

tampered with in anyway. A student may be charged up to the full replacement cost of the device for tampering with a school asset tag logo or turning in a device without a school asset tag.

Appropriate Content: All content must be school appropriate. Inappropriate materials include explicit or implicit references such as but not limited to:

- Alcohol, tobacco or drugs
- Gangs
- Obscene language or nudity
- Bullying or harassment
- Discriminatory or prejudicial behavior

Examples of <u>Unacceptable</u> Use: Unacceptable conduct includes but is not limited to:

- Proxy use to circumvent the firewall under any circumstances.
- Attempting to access or accessing sites blocked by the internet filtering system
- **"**Gaming"- Any game should serve an educational purpose.
- Using the network for illegal activities, including copyright or contract violations
- Unauthorized downloading/installation of any software including shareware and freeware
- Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments.
- Vandalizing and/or tampering with equipment, programs, files, software, network performance, or other components of the network; use or possession of hacking software is strictly prohibited.
- Gaining unauthorized access anywhere on the network
- Revealing the home address or phone number of ones'self or another person
- Invading the privacy of others
- Using another user's account or password, or allowing another user to access your account or password
- Coaching, helping, observing or joining any unauthorized activity on the network
- Posting anonymous messages or unlawful information on the network
- Participating in cyber-bullying or using objectionable language in public or private messages- e.g.- racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous
- Falsifying permission, authorization or identification documents
- Obtaining copies of, or modifying files, data or passwords to other users on the network
- Knowingly placing a computer virus on a computer or network
- Downloading music, games, images, videos, or other media without the permission of a teacher
- Sending or forwarding social or non-school related email

Technology Violations
Chronic, tech-related violations (see above)
Deleting browser history
Making use of the electronic resources in a manner that serves to disrupt the use of the network by others
Unauthorized downloading or installing software
Attempts to defeat or bypass the district's internet filter
Modification to district browser settings or any other techniques designed to avoid being blocked from inappropriate content or to conceal internet activity

Webcam: Each student device is equipped with a webcam. This equipment offers students an extraordinary opportunity to meet with teachers and classmates virtually.

Examples of use: Required digital class meetings, recording videos or taking pictures to include in a project, recording a student giving a speech and playing it back for rehearsal and improvement.

Inappropriate Use: The use of cameras without the direction of a teacher is strictly prohibited. Students should never hold or attempt to hold student-sponsored "live meetings." The use of cameras in public areas (including the bus) is strictly prohibited.

Please note inappropriate use of the webcam could result in disciplinary consequences.

Device Use and Care: Students are **prohibited** from:

- Defacing SD4 issued equipment in any way. This includes, but is not limited to: marking, painting (including fingernail polish), drawing or marring any surface or any stitching on the case.
- Removing SD4 stickers or adding personal stickers or additional markings on the devices, cases, batteries, or power cord/chargers.
- Using devices while food or drink are near.

Collection of District Owned Devices: The student's district-owned device and power adapter must be returned during a device check-in day, which will be set by the school. If a student transfers out of the school/district during the school year, the device must be returned to the school at the time of the transfer. If the device and/or power adapter and cord has been damaged or defaced, the parent/guardian could be charged additional fees. Failure to turn in the district-owned device will result in the student being charged the full replacement cost. The district may file a report for stolen property with the local law enforcement agency.