Spartanburg School District Four

Access to Digital Devices and Internet for Learning

2020-2021

Overview

Spartanburg School District Four views the use of electronic resources as an avenue that promotes ethical and responsible conduct in all electronic resource activities. With this privilege comes responsibilities for the parent and student.

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

SD4 students must understand that:

- The term "equipment" or "technology" refers to devices, batteries, power cord/chargers, and cases. Each piece of equipment is issued as an educational resource. The term "device" includes iPads, Laptops, Chromebooks and T-Mobile hotspot Mifi devices.

- Each T-Mobile hotspot Mifi device comes with a monthly plan of high-speed data that should be used for the sole purpose of promoting educational learning.

- All devices are on loan to students and remain the property of SD4.

- All users of the SD4 network and equipment must comply at all times with Spartanburg School District Four Board Policy IJNB. http://www.spartanburg4.org/departments/district_administration/policy_manual

- All users are accountable to school, district, local, state, and federal laws.

- Use of the devices and Internet must support education. Internet access is filtered for CIPA compliance on both devices and the mobile hotspot.

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

- All rules and guidelines are in effect for all SD4 devices whether on or off school campus.

- All files stored on SD4 equipment, the network, or cloud services are property of the district and may be subject to review and monitoring.

- Students are expected to keep the devices in good condition. Failure to do so may result in charges for repair or replacement.

- 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.

- Students are expected to notify their teacher or virtual school staff member 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 issued device or hotspot for any reason.

- Any failure to comply with the guidelines in this document may result in disciplinary action. SD4 may remove a user's access to the network without notice at any time if the user is engaged in any unauthorized activity.

- SD4 reserves the right to confiscate the property at any time.

Parent/Guardian Responsibilities

Sign the Student/Parent Technology Devices Agreement

Parent/Guardian Responsibility

In order for students to be issues a device, a student and their parent/guardian must sign the Student/Parent Technology Devices Agreement.

The parent/guardian/student are responsible for the cost of repair or replacement if the property is:

- Damaged-accidentally or intentionally.
- Lost because of negligence.
- Stolen, but not reported to school and/or police in a timely manner.

Monitor Student Use

Parent/Guardian Responsibility:

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.

Suggestions:

- Internet access on Devices and through the Hotspot Mifi Device are already filtered for CIPA compliance at school and away from school.
- Develop a set of rules/expectations for device use at home. Some websites provide parent/child agreements for you to sign.
- Only allow device use in common rooms of the home (e.g. living room or kitchen) and not in bedrooms.
- Demonstrate a genuine interest in what your student is doing on the device. Ask questions and request that they show you his or her work often.

Device Rules and Guidelines

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

Electronic Resource Policy and Responsible Use Procedures

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

- Support learning
- Follow local, state, and federal laws
- Be school appropriate

Security Reminders

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

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

Device Use and Care

Prohibited Actions

Students are prohibited from:

- Defacing SD4 issued equipment in any way. This includes, but is not limited to, marking, painting, drawing or marring any surface of the devices 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.

Troubleshooting

Troubleshooting Procedure

- Student tries to fix the problem.
- Try restarting the device.
    - If restarting the device doesn't alleviate the problem, please contact your summer school teacher.

Webcam

Purpose

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

Webcams are to be used for educational purposes only, by the direction of a teacher. Examples include:

Required summer school Zoom (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.

Important Note

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

Technology Discipline

Tech-related Behaviors	Equivalent "Traditional" Classroom Behaviors
Emailing, instant messaging, internet surfing, computer gaming (off-task behavior)	Passing notes, looking at magazines, games (off- task behavior)
Cyber-bullying	Bullying, harassment
Damaging, defacing, or endangering devices, accessories or files dangerous to the integrity of the network	Vandalism, property damage
Using profanity, obscenity, racist terms	Inappropriate language
Accessing pornographic material or inappropriate files	Bringing pornographic or other inappropriate content to school in print form
Using another person's digital account	Breaking into or using some else's locker

Tech Violations **Behavior unique to the digital environment without a "traditional" behavioral equivalent**
Chronic, tech-related behavior 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

Examples of <u>Unacceptable</u> Use

Unacceptable conduct includes, but is not limited to, the following:

- 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 one's self or another person
- Invading the privacy of other individuals

- 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 belonging to other users on the network
- Knowingly placing a computer virus on a computer or network
- Attempting to access or accessing sites blocked by the TCS filtering system
- Downloading music, games, images, videos, or other media without the permission of a teacher
- Sending or forwarding social or non-school related email

Device Security

Balanced Approach Two primary forms of security exist: device security and internet filtering. Each device has a security program installed. SD4 strives to strike a balance between usability of the equipment and appropriate security to prevent damage.

Device Security Security is in place on the device to prevent certain activities. These include downloading or installing software on the devices, removing software, changing system settings, 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 where the student is using the device. The T-Mobile hotspot Mifi device includes filtering software to ensure CIPA compliance for any device that connects to the Internet.

Damaged, Lost or Stolen Equipment

Damaged: If any equipment is damaged, the student must report it to their summer school teacher immediately.

Lost: If any equipment is lost, the student or parent must report it to their summer school immediately.

Stolen: If 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 and parent may be responsible for the cost of replacing the item(s) based on the chart below.

Replacement and Repair Costs

Financial Responsibility The circumstances of each situation involving damaged, lost or stolen equipment will be investigated individually. Students/families may be billed for damaged or lost equipment.

Chromebook Costs* *Damage fee applies for each occurrence	
Accidental Damage	**Intentional Damage**
Strike 1: Warning=$0 (loaner issued)	Strike 1: $25 (loaner issued)
Strike 2: $25 (loaner issued)	Strike 2: $50 (Per incident Determination)
Strike 3: $50 (Device returned)	
*Replacement Cost of Device: $300	

iPad Costs* *Damage fee applies for each occurrence	
Accidental Damage	**Intentional Damage**
Strike 1: Warning=$0 (loaner issued)	Strike 1: $25 (loaner issued)
Strike 2: $25 (loaner issued)	Strike 2: $50 (Per incident Determination)
Strike 3: $50 (Device returned)	
*Replacement Cost of iPad: $250.00 *Replacement Cost of a Cracked Screen: $75	

Laptop Costs* *Damage fee applies for each occurrence	
Accidental Damage	**Intentional Damage**
Strike 1: Warning=$0 (loaner issued)	Strike 1: $25 (loaner issued)
Strike 2: $25 (loaner issued)	Strike 2: $50 (Per incident Determination)
Strike 3: $50 (Device returned)	
*Replacement Cost of Laptop: $300.00	

Non-Warranty Damaged, Lost or Stolen Items	**Cost**
Power Adapter- All Devices (brick and cord)	$20.00
T-Mobile HotSpot Mifi Device and Charger	$50.00

Getting Started With the T-Mobile Mifi Hot Spot

What you will receive:

•T-Mobile Hotspot, Charging Cord and Charger Block

Turning on:

•Press the Power Side Button - you will see lights on the front come on.

•Do NOT press the ((WPS)) side of the button and do not press in the center of the button or the device will reset to factory settings.

When the Signal Bars and WiFi Active lights are on, your hotspot is ready.

Connecting your Chromebook:

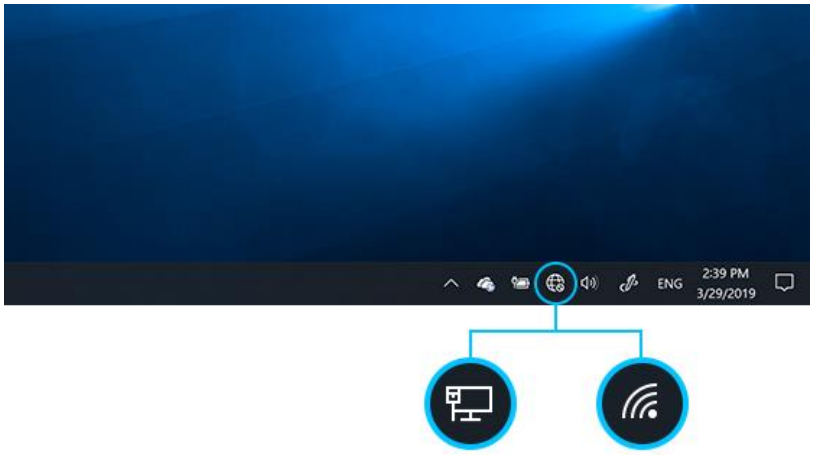
•With the hotspot on, you only need to boot up your Chromebook and it will connect automatically. If you open the 'Wireless Settings' - you will see that you are connected to 'THSMobile-Device#'.

Connecting your iPad:

- From your Home screen, go to **Settings** > Wi-Fi.
- Tap the T-Mobile Wi-Fi Hot Spot.
- Enter the password, then tap **Join**.

Connecting your Laptop:

- Select the **Network** icon on the taskbar. The icon that appears depends on your current connection state. If you do not see one of the network icons (or a similar one) shown in the following image, select the **Up arrow** to see if it appears there.



- Choose the T-Mobile network, then select “Connect”.
- Type the network password provided, then select “Next”.
- Choose No when asked to make the PC discoverable.

- T-Mobile tech support phone number: 1-844-361-1310