T-Mobile Wi-Fi Hotspot Checkout Agreement

Use of a hotspot is subject to the terms and conditions set forth in this checkout/access agreement, and by checking out the hotspot, you have agreed to the following:

- I understand that the hotspot can only be checked out by a student or staff member without existing access to the Internet at home and each must have a signed Wi-Fi Hotspot Checkout Agreement on file before a hotspot can be checked out.
- The assigned hotspot must be returned to the school district at the end of the school year, or upon approved request, with all included accessories, prior to leaving the district. Wi-Fi service will be disconnected, and the hotspot will no longer be usable if not returned. *Failure to return the device will result in an applicable replacement charge*.
- Hotspots must not be utilized at the school property, per ECF program rules.
- Wi-Fi service will be suspended if the hotspot is not being regularly utilized each billing month.
- Students and staff must not connect personal devices that are not provided by the district to the hotspot. Only devices provided by the school should be connected to the hotspot.
- Hotspots and the service are for educational purpose for the eligible student or staff member only and will not be sold, resold, gifted, or transferred.
- I understand and acknowledge that hotspots are unsecured, wireless networks and that any information being sent or received over the network could potentially be intercepted by another wireless user. Hotspot borrowers are cautioned against transmitting credit card information, passwords, and any other sensitive, personal information while using the wireless network. Due to this inherent insecurity, I agree that use of the hotspot is at the risk of the user/parent/guardian and agree to release and hold harmless the school, district, WV Department of Education and their board members, officers, employees, agents and representatives from any liability, damages, or expenses resulting from the use or misuse of the hotspot, connection of the hotspot to other electronic devices, or data loss resulting from the use of the hotspot.
- Students and staff using the hotspot must follow Policy 2460 Acceptable Use, which also prohibits students using devices to bypass state or vendor filtering. Also, as part of this policy, any use of the hotspot for illegal purposes, unauthorized copying of copyright-protected material in any format, or transmission of threatening, harassing, defamatory or obscene materials is strictly prohibited. I agree to comply with all applicable federal, state, and local laws, including those regarding obscenity, pornography and the delivery of any such material to minors, and state and district policies. I understand and acknowledge that the Internet contains images and content that may be offensive or harmful to myself or to others. I agree to release and hold harmless the West Virginia Department of Education (WVDE), district, school, and their board members, officers, employees, agents and representatives from all liabilities inclusive of, but not limited to those associated with the viewing of, use of or exposure to any information, picture, graphical representation or illustration that may be encountered while using the hotspot, regardless of whether the information appears on or is delivered through the device operated by the eligible student or staff member. I also understand that, while the hotspot and district-owned devices implement filtering software, nothing replaces parent/guardian monitoring and supervision of student access.
- The District reserves the right to require return by eligible students or staff members who abuse the hotspots. Damaged hotspots cannot be replaced by the district or WVDE. Any replacements will be at the cost of the parent/guardian or staff member.
- I understand that the hotspot runs on the Vendor network and that the speed and availability of the Wi-Fi connection will be dependent on the service area of the Vendor's towers. Service connection is not guaranteed in all areas.
- Students are subject to disciplinary action in accordance with district policy if inappropriate content is accessed

or posted. The student's use of the hotspot is subject to the Vendor's Acceptable Use Policy, Privacy Policy and Terms of Use, as well as WV State Policy 2460 and individual School District's Acceptable Use Policy. Students are bound by the District Acceptable Use Policy, school handbook, administrative procedure, and all other relevant guidelines, as well as the district County-Issued Device Usage Policy and Handbook wherever they use a hotspot and/or a Chromebook. I affirm that I have been provided the vendor COPPA Privacy Policy, CIPA Filtering documentation, and Technical Support documentation by the District and will review all contents.

- I understand that WVDE/School District are not responsible for any files, data, or personal information accessed, transmitted, lost or damaged while accessing the Internet via the hotspot.

By signing this agreement, I accept the above checkout agreement and am stating that I, as the parent/guardian, am responsible for returning this equipment to the School District in good working condition and free from damage.

School Name: _____

Student's Name (please print):_____ Grade Level:_____

Student's Signature:_____ Date:_____

Parent/Guardian Name (please print):_____

Parent/Guardian Signature:_____ Date:_____

Parent/Guardian Phone Number: _____

Parent/Guardian Email: _____

Parent Preferred Contact Method: Phone/Direct _☐__ Phone/Message_☐__ Email_☐__ Date_____

Hotspot # _____ Checkout Date _____ Due Date_____

Staff Use Only

Check Out: Please check to ensure that all pieces of equipment are present at the time of checkout.

☐ Hotspot ☐ Charging cable ☐ Instruction Card Staff Initials_____ Date_____

Check In: Please check to ensure that all pieces of equipment are present at the time of check in.

☐ Hotspot ☐ Charging cable ☐ Instruction Card Staff Initials_____ Date_____

COPPA Notice Addendum

T-Mobile is providing Customer with direct notice of its data collection, use and disclosure practices set forth below that relate to the Service(s). Customer has read this notice, consents on behalf of parents and guardians of children under 13 to the collection, use and disclosure practices described below, and authorizes T-Mobile to engage in such practices.

Direct Notice of T-Mobile's Data Collection, Use, and Disclosure Practices

We need your consent to collect personal information from your child(ren) in connection with the Project 10Million service. We will not collect, use, or disclose any personal information from children under 13 if you do not provide such consent. This privacy notice describes the personal information we collect and how we use it. The Federal Trade Commission has stated that a district or school may consent to such data collection, use, and disclosure on behalf of the parent or guardian to the extent such data collection, use, and disclosure is to provide services solely for the benefit of the school.

In addition to collecting student identification numbers for onboarding and verification purposes, T-Mobile intends to collect the following personal information from your child(ren):

- Data Usage: T-Mobile tracks quantity of broadband internet data usage to have that usage total counted against the 100 GB per year of free broadband internet access. As part of delivering this service, T-Mobile also receives the IP address associated with the websites visited.
- Unique identifiers: T-Mobile collects a device and network identifier to authenticate the device on our network and provide the service.
- Bandwidth data: T-Mobile may share device-level bandwidth data with the educational institution at the educational institution's specific request, to allow the educational institution to stay informed on devices that exceed applicable data usage/streaming limits.

T-Mobile uses this personal information only to provide internet connectivity and perform internal analytics. T-Mobile may disclose this personal information to its service providers for assistance in delivering the service, and they must treat this information as confidential and use it only for the purposes for which T-Mobile engaged them.

T-Mobile will not disclose information that may be associated with your child to any other entities.

Please be advised that T-Mobile provides connectivity to the general internet through the Project 10Million service. That connectivity allows children to access websites that may involve data collection by third parties. T-Mobile is not responsible for the data collection activities of these third parties and you should carefully monitor your child's use of the service.

TitanHQ WebTitan & T-Mobile CIPA Program 2020

Advanced DNS Web Filter With Real-Time Malicious Threat Detection and DNS web categorizations. Stop the risk of malware, ransomware, phishing and zero-day attacks before they harm your network. WebTitan is a vital web security layer for your business or school or home use.

CIPA is concerned with images and video content. To comply with CIPA, all images and video content of a pornographic or obscene nature must be blocked. That includes photographs, illustrations, cartoons, videos, and other graphics deemed to be obscene. Images of child abuse and child pornography must also be blocked.

Below is the CIPA filtering policy we apply to all T-Mobile CIPA clients:

Our CIPA compliance filtering addresses all of these issues for your school
We provide your school with the following:

Blocked Categories
These categories of websites are automatically blocked at source:

Anonymizer - Web pages that promote proxies and anonymizers for surfing websites with the intent of circumventing filters
Compromised - Web pages that have been compromised by someone other than the site owner, which appear to be legitimate, but house malicious code
Criminal Skills / Hacking - Activities that violate human rights including murder, sabatoge, bomb building, etc. Information about illegal manipulation of electronic devices, encryption, misuse, and fraud. Warez and other illegal software distribution
Hate Speech - Web pages that promote extreme right/left wing groups, sexism, racism, religious hate and other discrimination
Illegal Drugs - Web pages that promote the use or information of common illegal drugs and the misuse of prescription drugs and compounds
Mature - Sites not appropriate for children. Includes sites with content about alternative lifestyles, profanity, etc.
Nudity - Web pages that display full or partial nudity with no sexual references or intent
Phishing/Fraud - Manipulated web pages and emails used for fraudulent purposes, also known as phishing
Pornography / Sex - Explicit sexual content unsuitable for persons under the age of 18
Spam - Products and web pages promoted through spam techniques
Spyware and Malicious Sites - Sites or software that installs on a users computer with the intent to collect information or make system changes without the users consent.
Violence

Safe Search - SafeSearch helps keep adult & potentially offensive content out of your search results including image searches and web searches.
Safe Search is enabled automatically for **Google, YouTube, Yahoo and Bing**.

Any questions please reach out to your T-Mobile Rep.

Children's Privacy Notice | T-Mobile Privacy Center

We know it's important to treat data you tell us is from children under 16 carefully. This Notice explains what we do (and don't do) when it comes to children's data.

Just looking for our general Privacy Notice? You can find that here.

What Children's Data We Collect

We don't knowingly collect data from or about children without the permission of their parent or guardian. When we do collect that data, we might do it **directly**, like when you sign up for a service. We might also collect it **automatically** if your child uses the products or services we offer.

Different products and services collect different kinds of data:

Back to top

Kids' Privacy Setting - Kids' Lines

T-Mobile is currently testing the ability for parents and guardians to designate a line as a "kids' line." This feature enables parents to tell us that a line on their account is used by a child under the age of 16. Data from designated kids' lines won't be used for advertising and we'll opt the line out of receiving marketing communications from T-Mobile.

This feature is currently only available to T-Mobile customers, but we're working hard to expand access to all customers soon. In the meantime, customers can opt-out of the use of their data for advertising at any time through their account settings. We also have applied the opt-out to Project 10 Million, discussed further below.

We collect the following data from Kids' lines:

- **Geolocation Data –** we collect data that tells us the location of your child's mobile device.
- **Unique Identifiers –** we collect device and network identifiers – basically, ways for us to tell which mobile device on our network is your child's.
- **Age –** we collect your child's birth month and year so that we can tell when your child turns 16 and can change the line back to a regular wireless line.
- **Customer Proprietary Network Information ("CPNI")** generated by your child's use of our wireless voice communications services. See the CPNI article for more information.
- **Information from your child's use of our products, services, and network (and other carriers' networks when roaming domestically or internationally)** like usage of connecting carriers and Internet service providers, the Internet Protocol ("IP") address, text messages, and data use history, content interactions (e.g., how long you use an app), language

settings, and other network and device analytics and Wi-Fi connection and usage data.
- **Device and service performance and diagnostic information –** this includes reports from your child's device about signal strength, speeds, app and service performance, dropped calls, call and data failures, geolocation information, and device data.
- **Back-up information,** including data stored in back-ups and cloud services if your child's device uploads information to T-Mobile network servers (e.g., some devices may back-up the device's address book, photo album, or diagnostic data).
- **Audio information,** including voice commands your child provides to our apps (for example, for accessibility or hands-free use).

Read our Privacy Notice to learn more about how we collect, use, and share data from regular lines.

Back to top

Project 10 Million

Project 10 Million provides families that qualify with a free Wi-Fi hotspot and 100GB of free data. We collect the following data as part of Project 10 Million:

- **Child's first and last name.**
- **Child's Student ID –** we collect this to check whether your child is eligible.
- **Data Usage –** this tells us the amount of data the hotspot uses, and IP addresses associated with websites visited.
- **Unique Identifiers –** we collect device and network identifiers - basically, ways for us to tell which hotspot on our network is your child's.

Back to top

How We Use Children's Data

The main reason we collect children's data is to provide the product or service that collected the data. But we may also use children's data to do things like:

- Create and administer accounts, complete transactions, payments, billing, and requests related to our products and services and third-party products and services charged to your accounts.
- Check eligibility for a particular product or service.
- Help stop fraudulent, malicious, deceptive, abusive, or unlawful activities.
- Fix errors and ensure the quality, security, and safety of our products and services and network.
- Cooperate with law enforcement and protect the rights, safety, or property of our customers, T-Mobile and others.
- Comply with and enforce legal and regulatory obligations and respond to government requests.
- Enforce our policies, terms and conditions, or other agreements.
- Defend against or pursue claims, disputes, or litigation.

Back to top

When We Share Children's Data

Sometimes we hire others to help us provide a product or service, and these service providers may need access to children's data. They are required to keep children's data we provide them confidential and to use it only to provide the services we requested.

We may also share children's data with third parties, including the government, for legal processes or to protect life and safety where we believe that access, use, preservation, or disclosure of the data is reasonably necessary.

For Project 10 Million, we may also share aggregate versions of this data (meaning, data that cannot be associated with an individual child) with government agencies or schools.

Back to top

Your Rights as a Parent or Guardian

Parents and guardians have rights when it comes to their children's data:

- To change their mind and withdraw consent to the collection of their child(ren)'s personal data.
- To see the personal data T-Mobile has collected about their child(ren).
- To ask us to delete personal data T-Mobile has collected about their child(ren).

You can take any of these steps at the T-Mobile Privacy Center. We may need to collect some data from you to confirm you're the parent or guardian.

Important: We need to collect your child's data (as described above) to provide the relevant products or services. If you change your mind about giving consent or ask us to delete your child's data, the product or service may no longer work. **In some cases, the only way for us to stop your child's data from being collected might be to cancel your child's service.**

Back to top

For More Information

We're here to help.

- **Email:** privacy@T-Mobile.com
- **Toll-free Customer Service Number:** 1-800-T-Mobile (1-800-937-8997) or dial 611.

If you are unable to review or access this Notice due to a disability, please call us at 1-800-937-8997 or email us at privacy@T-Mobile.com so we can share it in another format.

Back to top

T··Mobile·

Tech Support to Parents and Students: 844-361-1310

Getting started: Franklin T9

Buttons and icons

There's a lot you can do with your new device, so here's a quick glance of some basic items to get you started.

1. **Power/Menu Button –** Turn on/off T9. Shows device menu and information

Button Operation

	Operations	Actions
⏻	Turn On	Press and hold the button for 3 seconds.
	Turn Off	Press and hold the button until "Goodbye" message appears.
	Display Wake-Up	When the display is off (sleep mode), the first quick press of the button wakes up the display.
	Info Display	When the display is on, press the button quickly to go through the device menu and information.

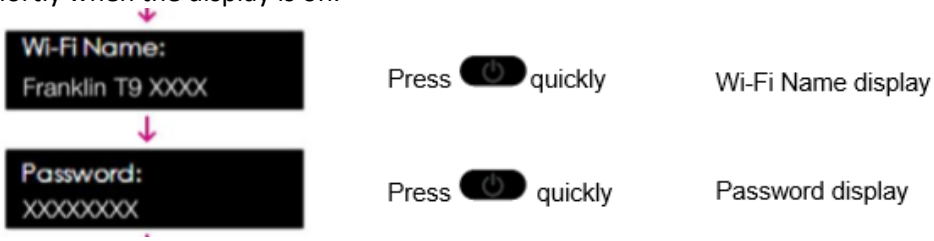
Device Display

First time use

When you first turn on your new device, you might see a setup wizard to help get you started. Look at the steps below to walk through the setup process. You can use your T9 as a wireless mobile hotspot to connect to a total of five Wi-Fi capable devices to the mobile broadband network.

Wi-Fi Name (SSID) and Password:

You can find your Wi-Fi Name and Password any time you need. Just press the power/menu button shortly when the display is on.



1. Power on your hotspot

   Press ⏻ quickly

2. Open the Wi-FI application or controls on your laptop or Wi-FI capable device that you want to connect to your T9. Then find your T9's Wi-Fi name.
3. Click **Connect** and enter the Password when prompted
4. Open your browser and you are good to go!