



Office of Procurement Services
8115 Gatehouse Road, Suite 4400
Falls Church, VA 22042

AMENDMENT NO. 17

08/15/2024

CONTRACT TITLE: Wireless Digital Voice & Data Services

| <u>CONTRACTOR</u> | <u>SUPPLIER ID</u> | <u>CONTRACT NO.</u> |
|--|---------------------------|----------------------------|
| AT&T Mobility II LLC dba AT&T Mobility National Accounts LLC PO Box 6463 Carol Stream, IL 60197 | 1000012319 | 4400011956 |

By mutual agreement, Contract 4400011956 is amended with the following:

- to add the AT&T Wireless Broadband Connectivity for Students service
- to update the supplier information per the table below

| From | To |
|--|---|
| Contract number: 4400011956 Supplier number: 1000012319 AT&T Mobility II LLC dba AT&T Mobility National Accounts LLC PO Box 6463 Carol Stream, IL 60197 | Contract number: 4400012909 Supplier number: 1000046330 AT&T DW Holdings, Inc. dba AT&T Enterprises, LLC 208 S. Akard St. Dallas, TX 75202 |

All other prices, terms and conditions of the Contract remain unchanged.

ACCEPTANCE:

BY:



Signature

Mark Flister

Printed Name

Sr. Contract Manager

Title

07/12/24

Date

DocuSigned by:



Michelle R. Pratt
Director

MRP/rt

DISTRIBUTION:

Contractor
FCG - DIT - Athena Baker

FCPS – Information Technology – Jean Welsh, Melissa York

EXHIBIT A

AT&T WIRELESS BRIDGING COMMUNITIES OFFER FOR STUDENTS

1. Connectivity Program for Students. The County has developed a program to enable students to obtain wireless broadband connectivity and connected devices (the “Connectivity Program for Students”), and Participant and Contractor intend to add provisions to the Contract to facilitate the Connectivity Program for Students by enabling the County to purchase Wireless Data Services and Equipment for use by such Students in accordance with the Bridging Communities Offer.

2. Bridging Communities Offer for Students – Description. Contractor has a bridging communities offer for students that includes certain Wireless Data Services and Equipment as described herein (the “Bridging Communities Offer”) The Bridging Communities Offer is not available to IRUs. In accordance with the Contract, the Bridging Communities Offer is subject to its underlying plan’s and equipment’s corresponding Sales Information, which is incorporated herein by reference. Pricing for the Bridging Communities Offer (a) is available for Student CRU lines for which the County has met the corresponding eligibility requirements; (b) is available for the corresponding offer period times set forth in §2 herein (the “Offer Period”); and (c) is subject to equipment availability. The Bridging Communities Offer is NOT eligible for the Service Discount, any other discount provided under the Contract, nor any other discounts or promotions otherwise available to AT&T’s customers. To the extent of any material conflict between the terms and conditions of this Exhibit A and the applicable Sales Information, this Exhibit A will control. Notwithstanding the foregoing, the Bridging Communities Offer is only available if the County’s account is active and in good standing with respect to the applicable CRU. For purposes of the Contract: (a) “Student” means an individual who is enrolled in an accredit non-profit educational institution; and (b) each Student is deemed to be a CRU. In addition to the provisions of this §2 below, with regard to County’s CRU lines for Students, the County is subject to the terms and policies described elsewhere in the Contract, including without limitation, the Acceptable Use Policy found at www.att.com/aup, the Privacy Policy found at www.att.com/privacy, and the applicable Sales Information for the Qualified Devices (as defined in §2.1.1. below) and Qualified Services (as defined in §2.1.2. below).

3. Bridging Communities Offer. Provided the County fully complies with the Contract, Contractor will make the Bridging Communities Offer available to the County and its eligible CRUs during the applicable Offer Period. The Bridging Communities Offer is being made in connection with the County’s Connectivity Program for Students.

3.1. Equipment and Services.

3.1.1. Use of Qualified Devices. The County may purchase the following Equipment for use by Students (each, a “Qualified Device”). The County must maintain title to each Qualified Device on which a Qualified Service is activated for so long as the Qualified Service is active on it.

| Promotional Qualified Device* | Equipment Price** | Offer Period | Eligibility Requirements |
|-------------------------------|-------------------|--------------|--|
| Franklin A10 (RT410) | \$0.00 | Initial term | During the Offer Period: <ul style="list-style-type: none"> Purchase the Qualified Device from Contractor with an Equipment Installment Plan 24 months or Custom 12-month term on the Unlimited throttled Data Connect Plan for a new CRU line of service for a Student; and Activate such new CRU line with Qualified Service (see §2.1.2 below). |

*Offer subject to Qualified Device availability.
 **Price does not include applicable taxes and may not be combined with other Equipment-related discounts or other offers.

3.1.2. Use of Qualified Services. The County must activate Qualified Devices with the following Plan(s) (each, a “Qualified Service”). The Qualified Services are provided to the County for the sole purpose of providing Students with wireless broadband connectivity for educational purposes. Each Qualified Service is subject to additional Service-specific pricing and terms set forth in the corresponding Sales Information, as modified by Contractor from time to time and which is incorporated herein by reference. Device, data, and speed restrictions may apply to certain Plans.

| Qualified Services | Offer Period | Eligibility Requirements | Sales Information* |
|--|--------------|---|---|
| AT&T Bridging Communities Unlimited Plan After 50GB, Contractor may temporarily slow data speeds if the network is busy. | Initial term | New CRU line of service for a Student with a Qualified Device | See Sales Information found at www.att.com/bcunl |
| AT&T Bridging Communities 10GB Plan | Initial term | New CRU line of service for a Student with a Qualified Device | See Sales Information found at www.att.com/bc10GB |

* Incorporated by reference into this Contract.

No other Services may be used in connection with the Connectivity Program for Students.

3.1.3. Recurring Credits on Select Qualified Services.

| Recurring Credit Amount | Qualified Service* | Offer Period | Eligibility Requirements |
|-------------------------|---|--------------|--|
| \$15.00/month | AT&T Bridging Communities Unlimited plan - see §2.1.2 (Use of Qualified Services) | Initial term | • County activates one or more new CRU line(s) of service for Students on the corresponding Qualified Service during the Offer Period (each, an “Eligible Line”); and • Each Eligible Line must continue to be on the corresponding Qualified Service at the time the Recurring Credit is applied** |
| \$10.00/month | AT&T Bridging Communities 10GB plan - see §2.1.2 (Use of Qualified Services) | Initial term | |

* Monthly pricing and terms are set forth in the applicable Sales Information, which is incorporated by reference into the Contract.
 ** Each Recurring Credit will appear on the applicable consolidated invoice as a per line credit applied to the monthly service charge before application of discounts, taxes, surcharges, and fees assessed on the Qualified Service. It may take up to 2 billing cycles after activation for the Recurring Credit to appear.

3.2. No Resale. The County and its Students (or their legal guardians, as applicable) are not permitted to resell, reproduce, retransmit, or disseminate the Qualified Services or Qualified Devices to third parties whether directly or indirectly including, without limitation, through machine-to-machine transmissions. In addition,

the County may not separately charge Students (or their legal guardians, as applicable) for all or a part the Qualified Services and Qualified Devices provided under this Contract.

3.3. Invoicing. The County will maintain all CRU lines for Students on foundation account(s) that are separate from the County's foundation account(s) with CRU lines for its Employees. Notwithstanding anything to the contrary elsewhere in the Contract, consolidated invoicing is the only invoicing method available for CRU lines for Students. Under consolidated invoicing, Contractor will provide a monthly invoice to the County that consolidates all charges incurred by Students under the foundation account for the preceding monthly billing cycle, except as may otherwise be noted in applicable online or printed terms and conditions of a Qualified Service. This monthly consolidated invoice is only accessible online through the County's online account management portal at www.att.com/premier. The County must promptly notify Contractor of any Numbers to be added or deleted from the County's consolidated invoice.

3.4. Additional Requirements.

3.4.1. Connectivity Program for Students - Terms of Use. The County has exclusive discretion and control over its Connectivity Program for Students, including, without limitation, determining individual eligibility, program purpose, and program terms, conditions, and restrictions. As a condition of allowing program access to the Qualified Services and Qualified Devices, the County will provide to each Student (or his/her legal guardian, as applicable) a set of County-branded terms and conditions governing the use of the Qualified Services and Qualified Devices that, at a minimum: (a) inform the Student (or his/her legal guardian, as applicable) of the County's privacy policy and data protection practices, (b) notify the Student (or his/her legal guardian, as applicable) that data associated with provision of the Qualified Services will be used exclusively for the purpose of providing the Qualified Services, (c) advise the Student (or his/her legal guardian, as applicable) that the Qualified Services and Qualified Devices are provided on an "as is" basis and that Contractor has no responsibility for the /Student's use of the Qualified Device or Qualified Services, and (d) indicate that Contractor is a third-party beneficiary entitled to all rights and benefits afforded to the County under the County's terms and conditions as if Contractor were a party to such terms and conditions.

3.4.2. Privacy. The County is exclusively responsible for any collection, use, sharing and ultimate deletion from the Qualified Devices of any data associated with use of the Qualified Device and/or Qualified Services by Students. To the extent the County engages in any return, trade in or device upgrade of a Qualified Device, the County will wipe the Qualified Device of data prior to such return, trade in or upgrade.

3.4.3. Notices and Consents. With regard to each Student participating in the County's Connectivity Program for Students, the County is exclusively responsible for providing any notices, and obtaining any consents, that are required by law. In addition, prior to distributing a Qualified Device to a Student that is under age thirteen (13), the County represents and warrants that the County will obtain from the Student's legal guardian all consents necessary for access to, and use of, the Qualified Devices and Qualified Services by the Student, including associated data as provided in §2.4.4.

3.4.3.1. Location-Based Notices. Third-party applications may allow the Qualified Devices used by Students to be location-enabled and thus tracked by the County. If the County loads any such device tracking application on a Qualified Device, the County is solely responsible for complying with all applicable legal requirements, including providing notice and obtaining opt in consent from the Student (or his/her legal guardian, as applicable), and the County will use such location information solely for the purpose of locating and retrieving Qualified Devices that are not timely returned to the County. Contractor will not collect, use, or otherwise have access to such location data, and the County will not provide such location data to Contractor for any purpose.

3.4.4. Data. The County will not provide to Contractor, nor will Contractor collect, use, or share, any personal information associated with access to or use of the Qualified Services and Qualified Devices by Students. Any data received by the County, or by Contractor in the course of providing wireless broadband connectivity to the County, relating to Students will be used exclusively to provide the Qualified Services, will not

be shared with third parties, and will not be used for any other purpose, including marketing or advertising.

3.4.5. Internet Safety Policy. The County represents and warrants that it has, and will maintain during the term of the Contract, an internet safety policy that addresses the following: (a) access by minors to inappropriate matter on the Internet and the World Wide Web; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access including "hacking" and other unlawful activities by minors online; (d) unauthorized disclosure, use and dissemination of personal information regarding minors; and (e) measures designed to restrict minors' access to materials harmful to minors.

AT&T Acceptable Use Policy

Notwithstanding any provision herein or elsewhere in Contract No. 4400011956, AT&T agrees to provide Fairfax County Public Schools ("Customer") with prompt notice and a reasonable opportunity to cure any purported violation of the attached Acceptable Use Policy ("AUP") and Privacy Policy before exercising any right it may have thereunder to suspend or terminate any Service to Customer (including Customer's end-users), except in those circumstances where, in AT&T's reasonable discretion, it determines that an immediate suspension or termination is necessary in order to protect Customer from network or system damage, or from legal liability. Any provision in the AUP and the Privacy Policy imposing liability obligations upon Customer for violations of the AUP and Privacy Policy will be enforceable if and to the extent permitted by applicable law, without waiver of FCPS sovereign immunity.

AT&T will not make any changes to the AUP, the Privacy Policy, or any other policy and terms ("AT&T Policies") during the term that will, individually or in the aggregate, materially and adversely impact Customer's use of the Services, or materially and adversely diminish AT&T's obligations to Customer and AT&T's end-users under Contract No. 4400011956, except to the extent expressly required under any laws, rules, or regulations applicable to the Services provided hereunder. In the event of a conflict between any other contract documents in Contract No. 4400011956 and any term or provision in an AT&T Policy, the documents as listed in the order of precedence from Contract No. 4400011956 will govern and control.

To be notified of changes to the Acceptable Use Policy, please complete the form available at <http://www.corp.att.com/aup/subscribe.html>.

Introduction

AT&T is at all times committed to complying with the laws and regulations governing use of the Internet, e-mail transmission and text messaging and preserving for all of its Customers the ability to use AT&T's network and the Internet without interference or harassment from other users. The AT&T Acceptable Use Policy ("AUP") is designed to help achieve these goals.

By using IP Service(s), as defined below, Customer(s) agrees to comply with this Acceptable Use Policy and to remain responsible for its users. AT&T reserves the right to change or modify the terms of the AUP at any time, effective when posted on AT&T's web site at www.att.com/aup. Customer's use of the IP Service(s) after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

Scope of the AUP

The AUP applies to the AT&T services that provide (or include) access to the Internet, including hosting services (software applications and hardware), or are provided over the Internet or wireless data networks (collectively "IP Services").

Prohibited Activities

General Prohibitions:

AT&T prohibits use of the IP Services in any way that is unlawful, harmful to or interferes with use of AT&T's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.

Failure to adhere to the rules, guidelines or agreements applicable to search engines, subscription Web services, chat areas,

bulletin boards, Web pages, USENET, applications, or other services that are accessed via a link from the AT&T-branded website or from a website that contains AT&T-branded content is a violation of this AUP.

Unlawful Activities:

IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule.

Violation of Intellectual Property Rights:

IP Service(s) shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of AT&T or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

Threatening Material or Content:

IP Services shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others. In addition, for those IP Services that utilize AT&T provided web hosting, AT&T reserves the right to decline to provide such services if the content is determined by AT&T to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libelous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others.

Inappropriate Interaction with Minors:

AT&T complies with all applicable laws pertaining to the protection of minors, including when appropriate, reporting cases of child exploitation to the National Center for Missing and Exploited Children. For more information about online safety, visit www.ncmec.org or www.att.com/safety.

Child Pornography:

IP Services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition may be reported to AT&T at the following e-mail address: cp@abuse-att.net. AT&T will report any discovered violation of this prohibition to the National Center for Missing and Exploited Children and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers.

Spam/E-mail/Usenet Abuse:

Violation of the CAN-SPAM Act of 2003, or any other applicable law regulating e-mail services, constitutes a violation of this AUP.

Spam/E-mail or Usenet abuse is prohibited using IP Services. Examples of Spam/E-mail or Usenet abuse include but are not limited to the following activities:

- sending multiple unsolicited electronic mail messages or "mail-bombing" – to one or more recipient;
- sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;

- sending unsolicited electronic messages with petitions for signatures or requests for charitable donations, or sending any chain mail related materials;
- sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of the AT&T network or of the networks with which AT&T interconnects, by virtue of quantity, size or otherwise;
- using another site's mail server to relay mail without the express permission of that site;
- using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUP;
- using IP addresses that the Customer does not have a right to use;
- collecting the responses from unsolicited electronic messages;
- maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the IP Services or the Internet (e.g., through language, frequency, size or otherwise);
- using distribution lists containing addresses that include those who have opted out;
- sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
- using redirect links in unsolicited commercial e-mail to advertise a website or service;
- posting a message to more than ten (10) online forums or newsgroups, that could reasonably be expected to generate complaints;
- intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;
- knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
- using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

Security Violations

Customers are responsible for ensuring and maintaining security of their systems and the machines that connect to and use IP Service(s), including implementation of necessary patches and operating system updates.

IP Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of AT&T's (or another

party's) server, network, network access, personal computer or control devices, software or data, or other system, or to attempt to do any of the foregoing. Examples of system or network security violations include but are not limited to:

- unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses;
- hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network;
- impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;
- distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
- engaging in the transmission of pirated software;
- with respect to dial-up accounts, using any software or device designed to defeat system time-out limits or to allow Customer's account to stay logged on while Customer is not actively using the IP Services or using such account for the purpose of operating a server of any type;
- using manual or automated means to avoid any use limitations placed on the IP Services;
- providing guidance, information or assistance with respect to causing damage or security breach to AT&T's network or systems, or to the network of any other IP Service provider;
- failure to take reasonable security precautions to help prevent violation(s) of this AUP.

Customer Responsibilities

Customers remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the IP Services. AT&T has no responsibility for any material created on the AT&T's network or accessible using IP Services, including content provided on third-party websites linked to the AT&T network. Such third-party website links are provided as Internet navigation tools for informational purposes only, and do not constitute in any way an endorsement by AT&T of the content(s) of such sites.

Customers are responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations.

AUP Enforcement and Notice

Customer's failure to observe the guidelines set forth in this AUP may result in AT&T taking actions anywhere from a

warning to a suspension or termination of Customer's IP Services. When feasible, AT&T may provide Customer with a notice of an AUP violation via e-mail or otherwise allowing the Customer to promptly correct such violation.

AT&T reserves the right, however, to act immediately and without notice to suspend or terminate affected IP Services in response to a court order or government notice that certain conduct must be stopped, or when AT&T reasonably determines that the Customer's use of the affected IP Services may: (1) expose AT&T to sanctions, prosecution, civil action or any other liability; (2) cause harm to or interfere with the integrity or normal operations of AT&T's network or networks with which AT&T is interconnected; (3) interfere with another AT&T Customer's use of IP Services or the Internet; (4) violate any applicable law, rule or regulation; or (5) otherwise present an imminent risk of harm to AT&T or AT&T Customers.

Copyright Infringement & Digital Millennium Copyright Act

AT&T respects the intellectual property rights of others. The Digital Millennium Copyright Act of 1998 (the "DMCA" found at 17 U.S.C. § 512) provides that owners of copyrighted works who believe that their rights under U.S. copyright law have been infringed may report alleged infringements to service providers like AT&T. In accordance with the DMCA and other applicable laws, AT&T maintains a policy that provides for the termination of IP Services, under appropriate circumstances, if Customers are found to be a repeat infringer and/or if Customers' IP Services are used repeatedly for infringement (the "Repeat Infringer Policy"). AT&T may terminate IP Services at any time with or without notice to Customers.

AT&T has no obligation to investigate possible copyright infringements with respect to materials transmitted by Customer or any other users of the IP Services. However, AT&T will process valid notifications of claimed infringement under the DMCA, and continued receipt of infringement notifications for Customer's account will be used as a factor in determining whether Customer is a repeat infringer. In addition, AT&T may voluntarily participate, on terms acceptable to AT&T, in copyright alert and graduated response programs.

Incident Reporting

Any complaints (other than claims of copyright infringement) regarding violation of this AUP by an AT&T Customer (or its user) should be directed to abuse@att.net. Where possible, include details that would assist AT&T in investigating and resolving such complaint (e.g., expanded headers, IP address(s), a copy of the offending transmission and any log files).

DMCA Copyright Notifications:

Pursuant to 17 U.S.C. §§ 512(b)–(d), a copyright holder may send AT&T a valid notification of claimed copyright infringement under the DMCA. For further information regarding such notifications, see <https://www.att.com/legal/terms.dmca.html>. AT&T's designated agent to receive notifications of claimed infringement as described in DMCA subsection 512(c)(3) is:

Registered Copyright Agent
4825 Creekstone Drive, Suite 300
Durham, NC 27703
E-mail: copyright@att.com

Due to the substantial volume of notifications of claimed infringement that AT&T receives and processes, we are unable to accept notices of alleged copyright infringement via this designated agent or email address other than notifications of claimed infringement

sent pursuant to Sections 512(b)–(d).

AT&T also provides transitory digital network communications services, pursuant to 17 U.S.C. § 512(a). In connection with such services, AT&T provides an online form that copyright holders should use to send notifications related to alleged copyright infringement by its users based on the standards of the Automated Copyright Notice System (ANCS). Copyright holders should use this online form to submit complaints related to alleged peer-to-peer file sharing (i.e. sharing media files via peer-to-peer networking technology), or other forms of copyright notice other than those sent pursuant to Sections 512(b)–(d) of the DMCA ("ISP Conduit Notices"). By submitting complaints using this online form, we are able to more efficiently manage and process ISP Conduit Notices. Due to the substantial volume of copyright notices that AT&T receives, we are unable to guarantee processing of ISP Conduit Notices that are sent by other means. Copyright holders can access AT&T's online form at att.com/p2pnotices. Please note that copyright holders must complete all fields in the online form before submitting.

Contact Information:

Any notification that AT&T sends to its Customers pursuant to this AUP will be sent via e-mail to the e-mail address on file with AT&T, or may be in writing to Customer's address of record. It is Customer's responsibility to promptly notify AT&T of any change of contact information.

Effective Date: July 28, 2017

AT&T Privacy Notice

Thank you for reading our Privacy Notice. Your privacy is important to you and to us. This notice explains how we use your information and keep it safe.

Importantly, it explains the choices you can make at any time about how your information may be used.

This notice applies to AT&T products and services including internet, wireless, voice and AT&T apps. We will tell you if a different notice applies. For example:

- Cricket and DIRECTV (including U-verse TV) have their own privacy notices.
- AT&T business customers may have a service agreement that covers the handling of information. The service agreement controls if it is different from this Privacy Notice.
- For AT&T business customers outside the United States, [the AT&T Business Customer Privacy Notice – Most of World](#) governs if different from this Privacy Notice.

Please make sure everyone who uses your account knows they are covered by this notice.

The information we collect

To better run our business, we collect information about you, your equipment and how you use our products and services. This can include:

- **Account information.** You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including [Customer Proprietary Network Information](#).
- **Equipment information.** We collect information about equipment on our network like the type of device you use, device ID, and phone number.
- **Network performance.** We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working.
- **Location information.** Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites.
- **Web browsing and app information.** We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information.
- **Biometric information.** Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our [Biometric Information Privacy Notice](#).
- **Third-party information.** We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.

All these types of information are considered Personal Information when they can reasonably be linked to you as an identifiable person or household. For instance, information is personal when it can be linked to your name, account

number or device.

How we use your information

We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we:

- Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers.
- Provide our products and services.
- Contact you.
- Improve your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care.
- Improve and protect our network.
- Use it to help understand which additional products and services may interest you and others. (We don't access or use the content of your texts, emails or calls for this or any other marketing and advertising.)
- Design and deliver advertising, marketing and promotional campaigns to you and others – and measuring their effectiveness ([See your choices](#)).
- Use it for billing, collection, and protection of our property and legal rights.
- Prevent and investigate security issues, illegal activities, and violations of our terms and conditions.
- Conduct research and create aggregated reports – reports that offer insights about groups of customers, but not individuals (we do not attempt to re-identify individuals in aggregated reports).

How we share your information

As described in the following paragraphs, AT&T shares information within our own AT&T companies and affiliates. We also share with non-AT&T companies.

AT&T affiliates. We share information that identifies you personally with our [affiliates](#), such as DIRECTV and Cricket. When we share this information, they must follow this Privacy Notice regarding your info, not just their own policy. This includes the [privacy choices](#) you make with AT&T.

AT&T affiliates and non-AT&T companies for advertising and marketing. We may share information with affiliates and other companies to deliver our ads and marketing or to assess their effectiveness. (Learn more about our ad programs and see [your choices](#).)

Non-AT&T companies providing a service. We use suppliers for services like marketing and mailing bills. When we

share your information with suppliers, we require them to use it only for the intended purpose and to protect it consistent with this notice.

Non-AT&T companies for identity verification. We share your information to protect you from fraud, authenticate your identity, protect your financial accounts and authorize transactions. When we share with companies like your bank for this purpose, we require them to use it only for the intended purpose and to protect it consistent with this notice. (Learn more and [see your choices](#), including your right to decline this service.)

Non-AT&T companies or entities where authorized or required by law. This can happen when we:

- Comply with court orders, subpoenas, and lawful discovery requests, and as otherwise authorized or required by law. Like all companies, we must comply with legal requirements. You can learn more in our [Transparency Report](#).
- Detect and prevent fraud.
- Provide or obtain information related to payment for your service.
- Route your calls or other communications, like connecting calls or text messages with other carrier networks.
- Ensure network operations and security, defend against legal claims and enforce our legal rights.
- Notify, respond, or provide information (including location) to an appropriate governmental entity in emergency circumstances such as immediate danger of death or serious physical injury.
- Alert the National Center for Missing and Exploited Children to information concerning child pornography if we become aware through the provision of our services.
- Share the names, addresses and telephone numbers of non-mobile phone customers with phone directory publishers and directory assistance services as required by law. We honor your request for non-published or non-listed numbers.
- Provide name and phone number for wireline and wireless Caller ID and related services like Call Trace.

Non-AT&T companies for metrics, insights and research. We may share aggregated (grouped) data that does not identify you personally for these purposes. We require that companies and entities agree not to attempt to identify individuals – or allow others to do so. We share in this manner for:

- **Metrics:** Sometimes you enjoy a service from us that directly involves another business. For instance, we might provide the Wi-Fi service at a place you visit. As part of our service, we may provide aggregate metrics reports to that business about how the Wi-Fi is being used, such as aggregated location and web-browsing data. It can only be used for group insights.
- **Insights:** We may share aggregated data about our network, operations or services.
- **Research:** We may share information for research. We require the entities to handle the data securely and not reuse or resell it.

Non-AT&T companies for location services. With your consent, we may share your location information for traffic and mapping apps and other location services to which you subscribe. We share only with your consent unless required by law. Keep in mind:

- You may give your consent to us, or you may give it directly to another company – like a medical alerting device company.
- If you give it directly to another company, that company governs the use or disclosure of location.
- In some cases, such as parental controls, consent may come from the AT&T account holder and not the individual user.

Your privacy choices and controls

You can manage how we use and share your information for certain activities including advertising and marketing. Here are key examples:

Do not sell or share my personal information. We may share information with other companies in limited ways, such as exchanging subscriber lists for joint marketing.

You can ask us to stop at any time, just:

- Visit att.com/PrivacyChoices or our [Choices and Controls page](#) and select “Do not sell or share my personal information.”
- Contact us at (866) 385-3193 if you are a California resident.

We recognize and honor the preference signal associated with a [Global Privacy Control](#).

Access, delete and correct your personal information. You can ask to see what personal information we have about you. You can also ask us to delete or correct it.

- **Access and Portability.** If you want to see the personal information we’ve collected, you can ask us for it. We will describe the categories of info we collect, the specific pieces we’ve collected, the sources of the information, the purposes for collecting, sharing or selling it and the categories of non-AT&T companies with whom we shared it. You can also ask to “port” your data, which means you get a copy that you can take with you.
- **Delete.** You can ask us to delete your personal information. In keeping with various state laws, please know that we will still keep data needed for things like running the business, security and fraud protection, compliance with legal obligations and marketing our products and services to our own customers.
- **Correct.** You can ask us to correct inaccurate personal information we have about you. We’ll ask you to provide documentation to support the correction and let you know the result.

To access, delete or correct your information, visit our [Choices and Controls page](#). California residents can also contact us at (866) 385-3193. Helpful details about the process can be found at [our Data Request Center](#), including your option to appeal.

We don’t mind if you make access, deletion or correction requests, or ask us not to sell or share information. These are rights under certain state laws, and we have extended their availability to others across the U.S., regardless of where you live.

As required by California law, you can review information specifically about California requests from the previous calendar year on our [California metrics page](#). We also follow state requirements within California regarding [businesses](#) and [those that provide work for us](#).

Personalized and Personalized Plus

AT&T has two programs that use your personal information to help customize your experience. For instance, you might be shown an online advertisement that is more relevant to your interests, rather than a general ad.

You can choose to participate or not – and it’s never a problem if you change your mind. You are automatically enrolled in the Personalized program, but you can always opt out. You must opt in to join Personalized Plus. Choices for both programs can be made at att.com/PrivacyChoices.

Here is a comparison of the programs:

| Data Use or Sharing Description | Personalized | Personalized Plus |
|---|--------------|-------------------|
| Uses data about your use of our products and services, including data from apps. | ✓ | ✓ |
| Uses demographic data like age range and ethnicity that we purchase from third parties. | ✓ | ✓ |
| Uses data from our advertising partners. | ✓ | ✓ |
| Uses automated decision-making, such as artificial intelligence. | ✓ | ✓ |
| Does not use information about your medical conditions or financial account information. | ✓ | ✓ |
| Does not access or use the contents of your texts, emails or calls. | ✓ | ✓ |
| May share data with other companies involved in advertising. | | ✓ |
| May use precise location and Customer Proprietary Network Information for marketing and advertising. | | ✓ |
| May use web browsing we collect as your internet provider for marketing and advertising and infer websites you visit over a secured connection. | | ✓ |

If you live in certain states, we won’t collect, use, store or share your sensitive personal information for marketing and advertising unless you join Personalized Plus. This includes information like ethnicity and racial origin. The states are

Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah and Virginia.

If you join the Personalized Plus program, it is an extension of the Personalized program, and you will be enrolled in both. If you also select a privacy option called “Do not sell or share my personal information,” you will be enrolled only in portions of Personalized Plus that don’t sell or share your information externally.

More choices and controls

Customer Proprietary Network Information (CPNI). CPNI is information related to the telecommunications services you purchase from us, such as which subscription plan you have and details about who you called. Your phone number, name and address are not CPNI. It is your right and our duty under federal law to protect the confidentiality of your CPNI.

You can choose whether we use your CPNI internally for marketing – such as helping to offer you new services and promotions.

You can opt out at att.com/cpni/optout. You can also call us any time at (800) 315-8303 and follow the prompts. Or you can talk to a service representative at (800) 288-2020 (consumer) or (800) 321-2000 (business).

We don’t share CPNI outside of our AT&T affiliates, agents and suppliers without your consent except for court orders, fraud detection, providing service, network operations and security, aggregate (grouped) information that doesn’t identify you personally and as otherwise authorized by law.


If you choose to restrict our use of CPNI, it won’t affect your services. We keep your choice until you change your mind, which you can do at any time. Keep in mind, even if you restrict use of your CPNI, you may still get marketing from us.

Identify verification. Non-AT&T companies like your bank may receive limited information from us to help protect your accounts from fraud, verify your identity and make sure it’s really you authorizing a transaction. We do not allow these non-AT&T companies to use your information for any purpose except those services. You are generally enrolled through the non-AT&T company, but you can stop at any time through us. Text “STOP” to 8010 to turn off Identity Verification, or text “RESUME” to restart. Or manage your choices at att.com/PrivacyChoices.

Contact preferences. We like to tell you about offers and programs that may interest you. You can manage how we do that. Keep in mind that we still may need to contact you with service and non-marketing messages. Please visit [Contact Preferences](#) for more information and links.

Industry choices and controls

Online behavioral advertising. You have industry-wide choices about online, interest-based advertising. Companies including AT&T may use cookies, mobile advertising identifiers, and other technologies to collect information about your use of websites including ours. This information can be used to analyze and track online activity or deliver ads and content tailored to your interests.

You can opt out of online behavioral advertising from companies that participate in the [Digital Advertising Alliance](#). Go to their [Consumer Choice Page](#). You can also select this icon  when you see it on an online ad.

- You can limit collection of data on websites by [managing cookies and similar technologies](#) on your computer. Remember that if you change computers, devices, or web browsers, or if you delete cookies, you will need to manage them again.

At AT&T, please note that when we collect web browsing information as an internet service provider, it works independently of your web browser’s cookie and private browsing settings that interact with online behavioral advertising. You can manage AT&T’s use of web browsing information – such as our Personalized Plus program – at att.com/PrivacyChoices.

We don't currently respond to Do Not Track. Please go to [All About Do Not Track](#) for more information. Unless you join our Personalized Plus ad program, we don't knowingly allow non-AT&T companies to collect your personally identifiable activity on our websites for their own use and tracking.

Data retention and security

We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like what type of personal information it is, how long it's needed to operate the business or provide our products and services, and whether it's subject to contractual or legal obligations. These obligations might be ongoing litigation, mandatory data retention laws or government orders to preserve data for an investigation. After that, we destroy it by making it unreadable or indecipherable.

We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.

No security measures are perfect. We can't guarantee that your information will never be disclosed in a manner inconsistent with this notice. If a breach occurs, we'll notify you as required by law.

Other privacy information

Information that we collect and share – in chart format

[This chart](#) shows the personal information that we collect, along with the purpose for its collection.

[This chart](#) shows the personal information we shared or sold over the past year about at least some consumers. It also shows the purpose for which we shared or sold it. Some states define "sale" very broadly.

[This chart](#) shows the sensitive personal information we've collected about consumers over the past year, including the purpose for its collection, sharing and sale.

Changes in ownership or to the notice

Information about you may be shared or transferred if AT&T is part of a merger, acquisition, sale of company assets or transition of service to another provider. Information could also be shared in the unlikely event that our business became insolvent, bankrupt or put into receivership.

We update this Privacy Notice as necessary to reflect business changes and satisfy legal requirements. We post a prominent notice on our websites of any material changes. We give you reasonable notice before any material changes take effect.

Information specific to business customers

We don't use our business customers' user information for marketing or advertising, except to market business products and services, including apps and devices. However, we may use our relationship with you to qualify you for certain deals on consumer products and services. You can call the toll-free number on your bill to see whether your current products and services are billed as business or consumer.

Information specific to children

We don't knowingly collect personal information from anyone under 13 without parental notice, and we get parental consent where appropriate. We also won't contact a child under 13 for marketing purposes without parental consent. However, if we are not aware that a child is using a service or device purchased by an adult, we may collect the information and treat it as the adult's. (See [your privacy choices](#).)

We don't have knowledge that we sell the personal information of anyone under 16. If we collect personal information that we know is from anyone under 16, we won't sell it unless we receive affirmative permission to do so. If a child is under 16 and at least 13, the child may provide the permission.

How to contact us about this notice

You can contact us with questions about this notice at privacypolicy@att.com. You can also write us at AT&T Privacy Notice, Chief Privacy Office, 208 S. Akard, Room 2901, Dallas, TX, 75202.

If you have questions not related to privacy, click on the "Contact Us" link on the bottom of any att.com page. It includes customer service numbers and links to chat and customer forums.

You can access your online account from the upper right-hand corner of our home page at att.com.

If you're not satisfied with our resolution of any dispute, including privacy and personal information concerns, you can learn about our dispute resolution procedures on our [dispute resolution page](#).

You also have the option to file a complaint with the FTC Bureau of Consumer Protection using an [online form](#) or calling toll-free to 877.FTC.HELP ((877) 382.4357; TTY: (866) 653.4261). Other rights and remedies also may be available to you under federal or other laws.



Financial Services
Office of Procurement Services
8115 Gatehouse Road, Suite 4400
Falls Church, VA 22042

6/24/2025

AMENDMENT NO. 18

CONTRACT TITLE: Wireless Digital Voice & Data Services

CONTRACTOR
AT&T DW Holdings, Inc.
dba AT&T Enterprises, LLC
208 S. Akard St.
Dallas, TX 75202

SUPPLIER ID
1000046330

CONTRACT NO.
4400012909

By mutual agreement, Contract 4400012909 is amended to renew for one (1) year effective July 1, 2025 through June 30, 2026. This is the fifth and final renewal option of five.

All other prices, terms and conditions remain unchanged.

ACCEPTANCE:

BY: 
Signature
Mark Flister
Printed Name

Sr. Contract Manager
Title
06/03/2025
Date

DocuSigned by:

Michelle R. Pratt
Director

MRP/rt

DISTRIBUTION:
Contractor
FCPS – Risk Management – Certificates@fcps.edu