

FLARE 

IQ **MACHINES**
Smart Technology for the MDU Environment

Flare Tempe
Internet Service
Information Packet

IQ Machines welcomes you to Flare Tempe. Like the other amenities provided by the property, the Internet service is a cut above – Flare Tempe has partnered with IQ Machines to deliver a superior Internet experience. Your Internet connection is powered by a dedicated fiber-optic network designed specifically for Flare Tempe. Connecting your devices to the network is simple, and you will enjoy ultra-fast data service across the entire property.

Getting Connected

Your Internet connection at Flare Tempe uses a username and password to connect your devices. Your credentials will allow you to connect phones, laptops, tablets, and computers directly to the "Flare" Wi-Fi network.

Some devices — such as smart TVs, gaming consoles, streaming devices, and printers — may not support username and password authentication. Instructions for connecting these devices are included below.

During the move-in process, you will receive an internet activation email from "portal@iqmachines.com". This email will be sent to the email address you have on file with the leasing office. Please be sure to check all folders in your email, including spam and junk. If you no longer have access to this email address or need to change it, please visit the leasing office for assistance.

The activation email will include your unique password and instructions for getting connected. This password is unique to your household and should not be shared with other residents.

All apartments and amenity areas at Flare Tempe are equipped with wireless access points broadcasting the "Flare" network. Once you connect your devices to the Wi-Fi network, they will reconnect automatically each time you return to Flare Tempe. Your devices will also work seamlessly as you move throughout the property — whether you are in your unit, an amenity area, or a neighbor's unit.

When connecting to the Flare Wi-Fi network, you will be presented with a certificate from our central authentication server. Please ensure you accept or trust this certificate when connecting your device. Otherwise, your device may fail to join the network.

Though uncommon, some devices, such as Android, may ask you for additional information when connecting to Flare Wi-Fi such as the EAP method and certificate selection. In this case, please use the following settings:

EAP method: PEAP

CA Certificate: None/Don't validate

Identity: Your username
Password: Your password

Connecting Devices That Do Not Support Username and Password

There may be cases where a device supports username and password authentication but still fails to join the network for various reasons. In this case, we recommend following the instructions below and registering those devices for the PSK network.

Some devices — such as TVs, game consoles, streaming devices, printers, and digital assistants — will require you to first add the device's unique wireless MAC address to the network before the device will connect to the Flare network. Using our website below, you will be able to add your own devices to the Flare network. Please note that this process is only required for devices that will not connect to Flare Wi-Fi using your regular username and password.

Visit <http://flaretempe.iqmachines.com> and sign in with your username and password. Please note that this is the same username and password you use to connect to Flare Wi-Fi. After inputting the wireless MAC address of your device to the website, please connect that device to the Wi-Fi titled Flare PSK and use the word "password" as the password.

Additionally, some devices have a "Randomized MAC Address" or "Private Wi-Fi Address" feature. This feature must be disabled for the device to work on the PSK network properly. If you are unfamiliar with disabling this feature, you may need to contact your device manufacturer.

Connecting to Other Devices in Your Unit

Once you connect a device to the Wi-Fi network using your password, you will be able to connect that device to other devices in your apartment. For example, you can connect your phone or computer to a printer, or cast video to a TV — as long as both devices are connected to the network using credentials associated with your apartment.

Your privacy is always maintained. Regardless of your location at the property, internet traffic from devices associated with your apartment is always separated from network traffic from other apartment units.

Important: Please do not connect personal routers or network equipment to the network. Your apartment is already equipped with enterprise-grade wireless access points designed to

provide full coverage. Personal routers will interfere with your connection and may affect your neighbors' connections as well.

Using Wired Connections

In addition to the Wi-Fi network, your apartment is equipped with wired Ethernet jacks in the Living Room that allow a direct physical connection to the network. These jacks are designed to connect your device automatically if it is configured with default network settings. Any devices connected to wired jacks in your unit will be accessible to other devices associated with your apartment that are connected to Wi-Fi.

Acceptable Use

Please note that your use of this Internet connection must comply with IQ Machines' Acceptable Use Policy, which is provided on the last page of this packet.

Support

Before contacting us, try these quick steps:

- Restart your device
- Make sure you are connected to "Flare" (not a neighbor's network)
- Double-check your username and password for typos
- Try "forgetting" the network on your device, then reconnecting
- If prompted for a certificate, make sure you accept or trust it

These steps resolve most connection issues within minutes.

What if my device still does not connect?

The Internet connection at Flare Tempe is designed to connect your devices automatically using default network settings. If your connection is still not working after trying the steps above, check that:

1. The wireless network connection on your device is enabled.
2. If using Wi-Fi, you are connected to "Flare" and are using the correct username and password.
3. If your device asked for EAP settings, verify they match: EAP method = PEAP, CA Certificate = None/Don't validate.

If your device still will not connect using your username and password, try registering it via the MAC address process described above. If you are still having trouble, please contact us — we're happy to help.

Contact Us

Support Hours:

Mon–Fri: 9 AM – 9 PM EST

Sat–Sun: 9 AM – 5 PM EST

Website: <https://iqmachines.com/find-your-complex/support-request/>

Phone: (480) 400-5200

Email: support@iqmachines.com

When contacting us, please provide:

- Your name
- A phone number or email where you can be reached
- Your property name and city
- Apartment number
- A brief description of the problem

Manage Your Account

You can manage your internet account — including changing your password — at any time by visiting:

<http://flaretempe.iqmachines.com>

Log in with your credentials to make changes to your account.

Acceptable Use Policy

This Acceptable Use Policy applies to all persons and entities (collectively, "customers") using the products and services of IQ Machines LLC ("IQ Machines") including Internet service. The policy is designed to protect the security, integrity, reliability, and privacy of both the IQ Machines network and the products and services IQ Machines offers to its customers. IQ Machines reserves the right to modify this policy at any time, effective immediately upon posting of the modification. Your use of IQ Machines' products and services constitutes your acceptance of the Acceptable Use Policy in effect at the time of your use. You are solely responsible for any and all acts and omissions that occur during or relating to your use of the service, and you agree not to engage in any unacceptable use of the service.

Prohibited Uses

Unacceptable use includes, but is not limited to, any of the following:

1. Posting, transmission, re-transmission, or storing material on or through any of IQ Machines' products or services, if in the sole judgment of IQ Machines such posting, transmission, re-transmission or storage is: (a) in violation of any local, state, federal, or non-United States law or regulation (including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations); (b) threatening or abusive; (c) obscene; (d) indecent; or (e) defamatory. Each customer shall be responsible for determining what laws or regulations are applicable to his or her use of the products and services.
2. Installation or distribution of "pirated" or other software products that are not appropriately licensed for use by customer.
3. Resale of IQ Machines' products and services without the express prior written consent of IQ Machines.
4. Deceptive marketing practices.
5. Actions that restrict or inhibit anyone — whether a customer of IQ Machines or otherwise — in his or her use or enjoyment of IQ Machines' products and services, or that generate excessive network traffic through the use of automated or manual routines that are not related to ordinary personal or business use of Internet services.
6. Introduction of malicious programs into the IQ Machines network or servers or other products and services of IQ Machines (e.g., viruses, Trojan horses and worms).
7. Causing or attempting to cause security breaches or disruptions of Internet communications. Examples of security breaches include but are not limited to accessing data of which the customer is not an intended recipient, or logging into a server or account that the customer is not expressly authorized to access. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information.

8. Executing any form of network monitoring that will intercept data not intended for the customer.
9. Circumventing user authentication or security of any host, network or account.
10. Interfering with or denying service to any user other than the customer's host (e.g., denial of service attack).
11. Using any program/script/command, or sending messages of any kind, designed to interfere with, or to disable a user's terminal session.
12. Failing to comply with IQ Machines' procedures relating to the activities of customers on IQ Machines-owned facilities.
13. Furnishing false or incorrect data on the order form contract (electronic or paper) including fraudulent use of credit card numbers or attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization or other methods to document "use" of IQ Machines' products or services.
14. Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, who were not previous customers of the customer or with whom the customer does not have an existing business relationship (e.g., E-mail "spam"); or distributing, advertising or promoting software or services that have the primary purpose of encouraging or facilitating unsolicited commercial E-mail or spam.
15. Harassment, whether through language, frequency, or size of messages.
16. Unauthorized use or forging of mail header information.
17. Solicitations of mail or any other E-mail address other than that of the poster's account or service, with the intent to harass or collect replies.
18. Creating or forwarding "chain letters" or other "pyramid schemes" of any type.
19. Use of unsolicited E-mail originating from within the IQ Machines network or networks of other Internet Service Providers on behalf of or to advertise any service hosted by IQ Machines or connected via the IQ Machines network.
20. Exporting, re-exporting, or permitting downloads of any content in violation of the export or import laws of the United States or without all required approvals, licenses and exemptions.
21. Hosting any services (for personal or business purposes) using IQ Machines network. The use of servers that enable services to be rendered to other users within or outside of the IQ

Machines network is prohibited.

No failure or delay in exercising or enforcing this policy shall constitute a waiver of the policy or of any other right or remedy. If any provision of this policy is deemed unenforceable due to law or change in law, such a provision shall be disregarded and the balance of the policy shall remain in effect.

Abusable Resources

Upon notification of the existence of an abusable resource (e.g., open news server, unsecured mail relay, or smurf amplifier), the customer shall immediately take all necessary steps to avoid any further abuse of such resource. Any abuse of an open resource that occurs after the customer has received such notification shall be considered a violation of this policy and enforced as such.

Enforcement

IQ Machines may immediately suspend and/or terminate the customer's service for violation of any provision of this policy upon verbal or written notice, which notice may be provided by voicemail or E-mail. Prior to suspension or termination, IQ Machines attempts to work with our customers to cure violations of this policy and ensure that there is no re-occurrence; however, IQ Machines reserves the right to suspend or terminate based on a first offense.

Electronic Communications Privacy Act Notice

IQ Machines makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon IQ Machines technology, and makes no guarantee that any other entity or group of users will be included or excluded from IQ Machines' network. In addition, IQ Machines may periodically monitor transmissions over its network for maintenance, service quality assurance or any other purpose permitted by the Electronic Communications Privacy Act, P.L. No. 99-508, as amended.

Questions?

If you are unsure of whether any contemplated use or action is permitted, please contact IQ Machines at support@iqmachines.com.