Arizona Culinary Institute Network Use Policy
Effective Date: 10/2025
Last Reviewed: 10/2025

1. Purpose
Arizona Culinary Institute ("ACI") provides access to its computer systems, networks, and internet resources to support its educational mission and administrative functions. This Network Use Policy establishes acceptable standards of behavior for anyone who accesses ACI's digital systems, Wi-Fi, or online services. Use of ACI's network resources signifies agreement to comply with this policy.

2. Scope
This policy applies to all students, faculty, staff, contractors, and guests who access:
• ACI's campus network (wired or wireless)
• ACI-issued computers, tablets, or mobile devices
• Email, cloud services, and software licensed by ACI
• Any system connected to or managed by ACI's IT infrastructure

3. Acceptable Use
Users are expected to use ACI's network and technology resources responsibly and primarily for legitimate educational or administrative purposes. Acceptable uses include:
• Conducting research, coursework, and institutional business
• Accessing academic resources or online training systems
• Communicating with ACI faculty, staff, and students for school-related activities
• Using email and internet services in a manner consistent with ACI's values and code of conduct

4. Prohibited Activities
The following activities are strictly prohibited on ACI's network:
• Accessing, downloading, or distributing obscene, illegal, or copyrighted materials without authorization
• Attempting to bypass or disable network security, firewalls, or content filters
• Engaging in hacking, phishing, or spreading malware or spam
• Using ACI's systems for commercial, political, or personal gain unrelated to academic activity
• Harassing, threatening, or discriminating against others online
• Sharing login credentials or using another user's account without authorization
• Connecting unauthorized hardware (e.g., personal routers, servers, or IoT devices) to ACI's network

Violations may result in disciplinary action, loss of network privileges, and/or legal consequences.

5. Security and Monitoring
ACI employs security measures including multi-factor authentication, endpoint protection, and continuous monitoring to safeguard institutional and personal data. Users should:
• Protect their passwords and change them regularly
• Report suspicious emails or cyber incidents to IT Support immediately
• Avoid connecting to unsecured public networks while using ACI accounts

All network activity may be logged and monitored for compliance, performance, and security purposes. Users should have no expectation of privacy when using ACI systems.

6. Data Privacy and Compliance
All network use must comply with:
• Family Educational Rights and Privacy Act (FERPA)
• Gramm-Leach-Bliley Act (GLBA) for safeguarding financial data
• U.S. Copyright Law
• ACI's Information Security Program

Personal and institutional data should only be stored or transmitted using approved ACI systems and encrypted connections.

7. Email and Communication Standards
All official communications with students, staff, and faculty should use ACI-issued email accounts. Users must:
• Use respectful and professional language
• Avoid sending mass or unsolicited messages not related to academic operations
• Refrain from sharing confidential information through unencrypted channels

8. Personal Devices (Bring Your Own Device – BYOD)
Personal devices may connect to ACI's guest or student Wi-Fi network, provided they meet security requirements:
• Device must have updated antivirus and operating system patches
• Device must not be jailbroken or rooted
• Users are responsible for the security of their personal devices

ACI reserves the right to restrict or disconnect any personal device posing a security risk.

9. Enforcement
Violations of this policy may result in:
• Revocation of network or system access
• Disciplinary action under student or employee conduct policies
• Notification to law enforcement or regulatory authorities, if applicable

10. Policy Review
This policy will be reviewed annually by ACI's Information Security Officer and updated as needed to align with regulatory, technological, or institutional changes.

11. Contact Information
For questions or to report security concerns, please contact:

Arizona Culinary Institute
Campus President
10585 N. 114th Street
Scottsdale, AZ 85259
Phone: (866) 294-2433
Email: info@azculinary.edu