I. SCOPE

This Acceptable Use Policy ("Policy") applies to all Authorized Users of Technology Resources at Arcadia University.

II. POLICY STATEMENT

Technology Resources support the mission of the University, as well as, all educational, instructional, research, and administrative activities. As an Authorized User of Technology Resources, you have access to valuable resources and sensitive data of the University. The use of Technology Resources is a revocable privilege extended to all members of the University community and it is vital for everyone to act in a responsible, ethical, honest, and legal manner when using Technology Resources.

The purpose of this Policy is to outline the acceptable use of Technology Resources at the University. The University is committed to ensuring open discourse and the free expression of viewpoints and beliefs. This commitment includes ensuring that academic dialogue is free from unwarranted institutional intrusion and oversight. With the values of open discourse and institutional restraint as guideposts, this Policy articulates and promotes the ethical, legal, secure, and acceptable use of Technology Resources by all members of the Arcadia University community and confirms the University’s responsibilities in connection with accessing such information.

Authorized Users of Technology Resources are responsible for ensuring that their activities adhere to the educational standards of the University’s educational mission. Within reason and in a manner consistent with the University’s educational mission, freedom of speech and unimpeded access to information will be honored.

III. POLICY

This Policy sets forth the standards by which Authorized Users may use Technology Resources. By using or accessing the University’s Technology Resources, Authorized Users agree to comply with this Policy and other applicable University policies that may be implemented from time to time, as well as all federal, state, and local laws, including copyright and licensing laws. Use of Technology Resources signifies your understanding and agreement with this Policy.
A. Acceptable Use: General guidelines for acceptable use of Technology Resources are based on the following principles and Authorized Users must:

1. Behave responsibly and respect the name of the University and the integrity and security of Technology Resources and the University network at all times.

2. Behave in a manner consistent with the University's mission and comply with all applicable laws, regulations, and University policies.

3. Be considerate and respect the rights and property of others, including privacy, confidentiality, and intellectual property.

4. Use computing resources for University related work.

5. Comply with security measures employed by the University and protect your account information from access by others.

6. Report violations of this Policy to the University’s Chief Information Officer or to the University’s Ethics Reporting System, which is managed by Navax Global and can found at https://secure.ethicspoint.com/domain/en/default_reporter.asp.

B. Unacceptable Use: Authorized Users are not permitted to:

1. Engage in any activity that is illegal under local, state, federal, or international law while utilizing Technology Resources. These include, but may not be limited to, child pornography, obscenity, harassing communications, software piracy, or threats of violence.

2. Violate the rights of any party or property protected by copyright, patent, or similar laws or regulations including, but not limited to, the unauthorized copying of copyrighted material including, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, Bit Torrent and other forms of Peer-to-Peer sharing of copyrighted information and the installation of any copyrighted software for which the University or the end user does not have an active license. Note, however, that it is not a violation of this Policy if the unlicensed use of the copyright protected work is done in accordance with the legal doctrine of Fair Use as defined in 17 US Code Section 107 of the Copyright Act of 1976.

3. Export software, technical information, encryption software or technology in violation of international export control laws or otherwise violate the University’s Export Control Policy found at http://www.arcadia.edu/export-control-policy.

4. Purposefully introduce malicious programs to the University’s network, computers, or storage areas (e.g., viruses, worms, Trojan horses, etc.).

5. Tap phone or network transmissions, including wireless transmissions.

6. Reveal your University account password or any other related passwords to others or allow use of your account by others. This includes family and other household members when work is being done at home.

7. Use Technology Resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
8. Use Technology Resources for private business, commercial or political activities, fundraising or advertising on behalf of non-University organizations or make fraudulent offers of products, items, or services originating from any University account.

9. Effect security breaches or disruptions of network communication.

10. Access data of which the Authorized User is not an intended recipient or log into a server or account that the Authorized User is not expressly authorized to access as a function of his/her University position. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinging floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Execute any form of network monitoring which will intercept data not intended for the Authorized User, unless this activity is a part of Authorized User's normal job or duty.

12. Circumvent user authentication or security of any host, network, or account.

13. Use any program, script, or command or send messages of any kind, with the intent to interfere with, or disable, a user's session.

14. Provide information about, or lists of, University employees or students to parties outside of the University other than FERPA compliant transactions.

15. Abuse email and internet activities, including, but not limited to:
   - Sending unsolicited email messages, junk mail, spam, or advertising material to individuals who did not specifically request such material;
   - Forging or the unauthorized use of email header information;
   - Discriminating on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability;
   - Sending, viewing, or downloading offensive content of any kind, including pornographic material or messages of a sexist, obscene, harassing, threatening, or racist nature;
   - Sending, viewing, or downloading messages of a religious or political nature for the purpose of proselytizing and/or soliciting funds or donations;
   - Creating or forwarding chain letters, Ponzi, or other pyramid schemes of any type;
   - Transmitting confidential or proprietary information; and
   - Gambling or any other activities that are illegal, violate any other University policy, or are contrary to the University's interest.

Authorized Users are responsible for the content of their email messages and should understand that others can use the content as evidence against them.

Any questions you may have as to whether your use of Technology Resources for academic, research, or educational purposes could violate the spirit of this Policy should be brought to the attention of your supervisor for prior approval.
C. Security and Proprietary Information

Using and/or accessing Technology Resources without proper authorization is strictly prohibited. All access is denied unless expressly granted. The University’s Information Technology Department generally grants access in the form of computer and network accounts to Authorized Users. Passwords and/or personal identification numbers protect University accounts. Authorized Users should use reasonable efforts to keep passwords secure and shall not share accounts. Passwords must be changed every 180 days. Additional information regarding this requirement can be found at: http://my.arcadia.edu/information-technology/computerservices/network-password. Authorized Users should also log out or lock their computer at all times when they are away from their computers, laptops, iPads, tablets, or other devices.

While the University does not generally monitor information transmitted over the University network, the University reserves the right to audit the network and related systems at any time for security and maintenance purposes and to comply with applicable laws. Accordingly, the University cannot guarantee the confidentiality of information stored on any University network device. For your protection, Authorized Users should not have any expectation of privacy with regard to communications passed through the network or stored on computers that use it.

For your protection please note the following:

Confidential information should be encrypted and may not be stored on a local hard drive or devices such as laptops, tablets, USB drives, or other devices that can fail or be lost or stolen. The University network drives must be used to store University related materials.

Authorized Users should exercise caution when opening e-mail attachments received from unknown senders, which may contain malicious codes.

Authorized Users are discouraged from storing any University information on publicly accessible cloud storage services such as a personal account on Google Apps, Dropbox, or Box.com. University data must be stored on Arcadia-owned accounts on these services.

Information not intended for the general public should be posted on the University’s intranet site, my.arcadia.edu, as opposed to the public website. Please contact the Office of University Relations for details regarding My Arcadia.

D. Enforcement

The University considers violations under this Policy to be serious offenses and will take such action it deems necessary to protect its network from events that threaten or degrade operations. The University reserves the right to disconnect or disable, without warning or prior notice, any computer, account, or service that poses a security or performance threat to University resources or services or that otherwise violates University policies. Access may be later restored after the incident has been reviewed and the risk mitigated or eliminated. Any Authorized User found to have violated this Policy may be subject to disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University or investigation and/or prosecution by the appropriate local, state, or federal authorities. University is not liable for the actions of anyone connected to the Internet through the Technology Resources. All users will assume full liability, legal, financial or otherwise, for their actions.
IV. DEFINITIONS

**Authorized Users** are all users of Technology Resources including, but not limited to, employees, temporary employees, faculty, students, alumni, campus visitors, contractors, vendors, consultants and their related personnel, and other users authorized by the University to access its systems and networks.

**Technology Resources** are assigned computer accounts, email services, and the shared University Network which includes resources and facilities operated by the University, whether owned, leased, used under license or by agreement, including, but not limited to: telephones (including mobile devices) and telephone equipment, voice mail, SMS, mobile data devices, desktop and laptop computers. Email, chat, facsimiles, mail, any connection to the University's network or use of any part of the University's network to access other networks, connections to the Internet that are intended to fulfill information processing and communications functions, communication services, hardware, including printers, scanners, facsimile machines, any off-campus computers and associated equipment provided for the purpose of University work or associated activities.

**University** is Arcadia University, its colleges, schools, affiliates, divisions and subsidiaries.

V. EFFECTIVE DATE

This Policy is effective on the date that it is approved by the President.

VI. SIGNATURE, TITLE, AND DATE OF APPROVAL

By: [Signature]

President, Arcadia University

Date: 6/20/16

Acceptable Use Policy
MMC M Drive
April 25, 2016