POLICY

ASCENT CHRISTIAN ACADEMY TECHNOLOGY ACCEPTABLE USE POLICY

NOTE: The school has a separate form to sign and return to the school office. You can find that form among the enrollment forms.
Every classroom at Ascent Christian Academy is equipped with access to the Internet. Ascent Christian Academy is committed to using this resource in a manner that is beneficial to students. Students will learn responsible use of the Internet as a valuable learning and collaborative tool, and will use the Internet to aid learning in all academic areas.

Introduction
Ascent Christian Academy has a commitment to provide programs for students to develop awareness, and a degree of proficiency, in the understanding and use of technology. Our goal is to integrate technology into a student's experience at ACA so that he/she can become a life-long learner and user of these resources. Our technological equipment is located in classrooms and in other specialized areas of the entire church campus. There has been an investment of funds in order to provide our students with the appropriate technological resources for their education. Desiring to be good stewards of God's provision for ACA, we have formulated this Acceptable Use Policy (AUP) for all persons involved in using school technology. As an overriding principle, we require those using school technologies, to exercise godly discernment and judgment, be willing to follow stated procedures, and show consideration to both the equipment and others in its usage. It is to be understood that there will be serious consequences for any inappropriate use, deliberate damage, or failure to follow directions in handling the equipment, including hardware, software, printers, scanners, cameras, etc. Willful destruction of school property is considered vandalism and will be dealt with in accordance with the ACA Discipline Code. In addition to appropriate discipline, restitution will be required for repairs or replacement of damaged equipment. Persons willfully or maliciously damaging, or violating this AUP will lose the privilege of using the school's technology in the future. Personal equipment from home may not be brought to school without expressed written permission from the administration.

About this Document
This document presents the technology acceptable use policy of Ascent Christian Academy. All users of ACA technology must use ACA technology in accordance with this policy. Separate policies and agreements exist for other aspects of technology use at ACA. This document contains several acronyms and italicized words or phrases. Definitions or descriptions of those acronyms, words, and phrases are provided in the last section.

Separate Policies & Agreements
Students, Faculty & Staff
ACA internet and email policy
Faculty & Staff Only
Faculty & Staff Addendum to AUP
ACA Website & Blogging Guidelines

Definitions & Descriptions

- **ACA:** Ascent Christian Academy
- **AUP:** Acceptable Use Policy
- **FTP:** File Transfer Protocol

- **SPAMMING:** Sending numerous copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or sending very large messages or files to a recipient that disrupts a server, account, newsgroup, or chat service.

General Guidelines

- All usage is not to violate existing copyright laws.
- All ACA technology equipment resides within the United States. ACA users are bound by U.S. laws concerning peer-to-peer file sharing networks.
- Any violation of this AUP is to be reported to ACA administration
- Installation of software of any kind on ACA clients or servers without express written permission from the director of technology is strictly prohibited.
- *Illegal Activity* is strictly prohibited.
- *Inappropriate content* is strictly prohibited.
- Violating the rules, regulations, policies, or terms of any network, server, computer database, or web site will be considered a violation of these policies.
- Removing ACA technology without the express written permission from the director of technology is strictly prohibited.
- Use of technology equipment owned by the school must be *normal and ordinary*

Security

- Each user is responsible for the security of his or her account.
- Passwords are to be kept confidential.
- Leaving a workstation unattended and logged-in is strictly prohibited.
- Locking a workstation without express written permission from the director of technology is strictly prohibited.
- Any user who suspects his or her account has been used by someone else must report this to ACA administration.
- *Circumventing* the security of any host, network or domain is strictly prohibited.
- *Cracking* is strictly prohibited.
- The use of laptops without express written permission of the director of technology is strictly prohibited.
- Wireless networking without express written permission of the director of technology is strictly prohibited.
- *Serving* without express written permission of the director of technology is strictly prohibited.

The User Community

- *Interfering* with the operation of any ACA technology, the ACA domain or any host, network or domain is strictly prohibited.
- Running automated tasks, unattended processes, bots, cron jobs, scheduled tasks, etc. without express written permission from the director of technology is strictly prohibited.
- Running any process, unattended or not, that is run simply for the purpose of hindering the operation of the ACA domain or any host, network or domain is strictly prohibited.
- Trespassing into other's folders, files, or work is prohibited.
- ACA technology is not to be used to harm other people or their work.

File Transmission & Data Storage

- Each user is responsible to know where to save files. The hard drives in most clients are regularly 'emptied' of files and folders. Saving work in the wrong place will result in data loss eventually.

- Anonymous FTP without express written permission from the director of technology is strictly prohibited.
- Binary files, including most kind of proprietary file formats (MS Word, Excel, etc.) must be transmitted via e-mail unless the user has express written permission of the director of technology to use another method.
- Transfer of images and executable programs by any means without express written permission from the director of technology is strictly prohibited.
- Use of *removable media* other than software purchased by ACA without the express written permission of the director of technology is strictly prohibited.
- All file and data transfer over the ACA network must be *normal and ordinary*.
- The transfer of *inappropriate content* is strictly prohibited.
- The preferred method of file transfer is e-mail.

Illegal Activity
Posting, storing, transmitting or disseminating information, data or material which is libelous, obscene, unlawful, threatening, defamatory, or which infringes the intellectual property rights of any person or entity, or which in any way constitutes a criminal offense, give rise to civil liability, or otherwise violate any local, state, federal or international law, order or regulation.

Inappropriate Content
Posting, storing, sending, transmitting, or disseminating any information or material which a reasonable person could deem to be objectionable, offensive, indecent, pornographic, harassing, threatening, embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful.

Removable Storage Media
Any medium used for the purpose of data storage and transport between computers and computer systems. This includes, but is not limited to, floppy disks, CDs, USB drives, flash drives, PDAs, phones, video, and digital cameras.

Circumventing
Accessing or attempting to access any host, network, domain, system, software, or data without proper authorization to do so; breaching the security of another user on any host, network, domain, or system; attempting to bypass the user authentication or security of any host, network, domain, system, server or client. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other hosts, networks, or accounts.

Cracking
Using or distributing tools designed or used for compromising security, such as password guessing programs, decoders, password gatherers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan horse programs; network probing; port scanning; or using or distributing programs that remove locks or time-outs built into software (cracks).

Interfering
Inhibiting, or otherwise disrupt the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the service of any host, network, domain, system, website, or database; posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to send or retrieve information; restricting, inhibiting, or otherwise disrupting or causing a performance degradation, regardless of intent, purpose, or knowledge, to any server, backbone network,

node or service; issuing denial of service attacks; port-flooding; improperly seizing administrator or root privileges; or attempting to “crash” a server or client.

Serving
Reselling or otherwise making available to anyone outside of ACA the services of the ACA domain in whole or in part; or accepting inbound requests from any other client. This includes, but is not limited to, operating your own HTTP, FTP, email, proxy or print server; offering Wi-Fi, Bluetooth, ad-hoc or other types of wireless connections to your client; sharing your files over the ACA network; running any kind of chat, talk, IRC, or IM service; or making your files available via peer-to-peer or distributed file sharing systems.

Normal and Ordinary
Any use of ACA technology or the ACA network that any reasonable person would find acceptable by faculty, staff, or students. Examples include, accessing the Internet for the purpose of developing lesson plans, completing a homework or classwork assignment, reinforcing a learning experience, or professional development.

The World Wide Web
The World Wide Web is the most common tool used for access to the Internet. It is a constantly changing environment and is becoming increasingly interactive. Parents and teachers must use extreme caution while encouraging students to make use of this resource for educational purposes. With this in mind, ACA has adopted the following guidelines for use of the World Wide Web.

- Students must not browse the web unless under the supervision of ACA faculty or a substitute teacher.
- ACA does not guarantee the availability, compatibility or suitability of outside networks or applications hosted on outside networks.
- Many websites prohibit use by children under a certain age. Students must observe these rules at all times.
- Use of the world wide web by minors under the age of thirteen and communicating with minors under the age of thirteen via the world wide web is governed by federal law. Students under the age of thirteen are not permitted to use web based forms or login to accounts of their own on any website.
- Teachers must not require students under the age of thirteen to provide any personal information in order to use a website or other service provided via the Internet.

Content Filtering
ACA provides access to the Internet for educational purposes. Unfortunately, the Internet also provides access to content that is objectionable, offensive and even harmful to students. ACA intends to protect students from objectionable content using whatever means available. Students and parents should be aware of the following:

- The ACA network is protected from intrusion using a firewall which is managed and monitored 24 hours a day.
- All access to the Internet at ACA is filtered using proxy services provided by the technology director.
- All content labeled as pornography or gambling is blocked for all users including faculty and staff.
- In addition to blocking objectionable, offensive and harmful content for all users, ACA also blocks student access to some content in order to enforce its *Technology Acceptable Use Policy* and *Internet & E-mail Use Policy*.

- ACA will resort to any means necessary in order to protect students from objectionable content. Our firewall is configured to deny all access to the Internet in the event of failure of proxy services.
- In the event of firewall failure, access to the Internet will be disabled by disconnecting classroom clients from the ACA network.
- ACA cannot guarantee that all objectionable, offensive or harmful content is filtered.
- Students are not permitted to use the Internet unless an ACA faculty member or substitute teacher is in the room.
- Students in grades K – 5 are not permitted to use the Internet unless directly supervised by an ACA faculty member or substitute teacher.

E-Mail

Use of e-mail on campus is permitted according to the following guidelines:

- Users over the age of twelve who have web-based access to personal e-mail may use it for personal use while on campus, but ACA will not provide support or guarantee the availability or suitability of any third party service.
- All users who use personal e-mail on campus must always adhere to the Terms of Service or Acceptable Use Policy of that service.
- All faculty and some staff members are given an official Ascent Christian Academy email address and are required to use it for school business.
- Each user is responsible for his or her own communication and the consequences thereof.
- Sending *Unsolicited Commercial E-mail* is strictly prohibited.
- Spamming is strictly prohibited.
- Sending unauthorized mail via open, third-party servers is strictly prohibited.
- Collecting, or attempting to collect, personal information about others without their consent is strictly prohibited.
- Selling, exchanging or distributing e-mail addresses to a third party is strictly prohibited.
- Participating in the collection of e-mail addresses, screen names, or other identifiers of others, or participating in the use of software designed for this purpose is strictly prohibited.
- Sending, uploading, distributing or disseminating or offering to do the same with respect to any unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, or otherwise objectionable content is strictly prohibited.
- Intentional distribution of viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature is strictly prohibited.
- Conducting or forwarding pyramid schemes and the like is strictly prohibited.
- Transmitting content that may be harmful to minors is strictly prohibited.
- Impersonating another person (via the use of an email address or otherwise) or otherwise
  misrepresenting yourself or the source of any email is strictly prohibited.
- Illegal transmission of another's intellectual property or other proprietary information without such owner's or licensor's permission, knowingly or unknowingly is strictly prohibited.
- Using email to violate the legal rights (such as rights of privacy and publicity) of others is strictly prohibited.
- Promoting or encouraging illegal activity is strictly prohibited.
- Use of Gmail, Outlook or any other mail user agent to send or receive POP/IMAP e-mail from ACA PCs is strictly prohibited. Users who would like access to POP e-mail must use a web based service that provides this.

- ACA employees may not reply to e-mails they believe to be from minors under thirteen years of age.
- ACA employees may reply to emails from ACA parents who are currently enrolled in ACA.
- An employee of ACA may reply to e-mails from his/her own children regardless of any other part of this agreement which might prohibit a reply.

All of the following will be considered *Unsolicited Commercial E-mail*:

- email that is in violation of the CAN-SPAM Act or any other applicable anti-spam law
- email sent to users who have requested to be removed from your mailing list or address book
- email sent to a significant number of email addresses belonging to individuals and/or entities with whom you have no preexisting relationship

Instant Messaging

The ports used for most instant messaging systems are blocked for security purposes. Users may use web based systems to access instant messaging systems in accordance with the following guidelines:

- All conversation participants must be thirteen years of age or older.
- Students may not use IM during class unless specifically instructed to do so by the teacher or substitute of that class during the same class period.
- Students may not participate in a conversation with any other participant who is in a class at ACA or any other school.
- School codes of conduct apply to all communication via instant messaging.
- Illegal activity is strictly prohibited.
- Spamming is strictly prohibited.
- Instant messaging is not to be used to harass others.