Parental Consent Form

Students involved in activities on-campus may need to use university-owned technology or take advantage of wireless internet access. All users, including guest users, have to be at least 16 years of age or older and have to agree to the attached official network user policy guidelines.

If the user is less than 16 years of age, it is required that a parent or guardian sign this parental consent form in order to receive university login credentials.

While on-campus, the faculty or staff member responsible accepts actions for the hosted guest(s).

Parent's Name _____

Child's Name _____

My child agrees to abide by the official Elon University Acceptable Usage Policy found below on pages 2-3 of this form. It can also be found on the technology website at:

https://www.elon.edu/u/bft/technology/forms-and-policies/policies/acceptable-usage/

My signature below indicates our acceptance of the terms of the policy.

_____ _____

Parent's signature Date

_____ _____

Supervisor's signature Date

Acceptable Usage Policy

1.0 Purpose

Elon University provides a wide variety of computing, networking, and other technology facilities in order to promote and support academic pursuits. Instructional & Campus Technologies maintains and supports computing and networking services as well as other technologies in support of the university's mission.

By using University technology, users agree to abide by the guidelines listed below. Additional policies may also apply to specific systems (such as email and Web) and are posted on the Technology Forms & Policies page. Any questions regarding this and other policies should be addressed to the Assistant Vice President for Technology.

2.0 Scope

This policy applies to all users of Elon University Technology.

3.0 Policy

3.1 Individual use

Your account and network connection are for your individual use. A computer account is to be used only by the person to whom it has been issued. You are responsible for all actions originating through your account or network connection. You must not impersonate others, misrepresent yourself, or conceal your identity in electronic messages and actions.

3.2 Respect the privacy and security of users and systems

Unless information is specifically made public or accessible to you, you should assume anything on the network is private. Just because you may have the ability, through a loophole, someone's carelessness, etc., to access files, directories, or information that does not belong to you, you do not have the right to do so. Any attempt to circumvent computer, network or file security, or to take advantage of security lapses is prohibited.

3.3 Do not disturb other users or abuse computer resources

Disruptive and/or invasive actions using computer systems and networks are strictly prohibited. Examples of this include, but are not limited to: viruses, threatening or harassing messages, "spamming," packet sniffing, self-perpetuating programs, excessive volume of file transfers, network traffic or printing and other programs, files, hardware, software or actions that deliberately or unintentionally degrade or disrupt system or network performance, compromise or circumvent system or network security, or interfere with the work of others. Due to its adverse impact on our systems and networks, the sending of chain letters and similar "passalong" email messages is explicitly prohibited.

3.4 Respect intellectual property

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments."[1] The burden of proof of ownership or obtaining permission from the copyright owner is upon the account holder. Upon receiving proper notification, as defined by the Digital Millennium Copyright Act, of a potential infringing activity, we will, where possible, remove or block access to the material in question. Reports of repeated copyright infringement will lead to termination of computer/network services and/or other university/legal actions.

[1] "Using software: A Guide to the Ethical and Legal use of Software for Members of the Academic Community," EDUCOM (Princeton, NJ, 1987).

3.5 Access to computer accounts and networks/Noncommercial use only

Elon University will make reasonable efforts to have its computer systems and networks available at all times. However, as part of regular maintenance and other planned and unplanned activities, systems and networks may be unavailable at any particular time. Elon University reserves the right to restrict or terminate access to its computer and network resources as necessary. Elon University computer systems, facilities and network resources are for noncommercial individual use related to the educational mission of the University by its faculty, staff and students, and for approved university business activities. Elon University reserves the right to limit or terminate access to computing, networking and other technology facilities as necessary.

3.6 Abide by the regulations: don't break the law

All users must abide by all university rules and policies, as well as local, state and federal laws. This includes, but is not limited to, other Instructional & Campus Technologies policies; other University policies; any local, state and federal regulations.

3.7 Safety

a. Online - You must be careful when you are online. The internet is accessible to everyone so you should take precautions to protect yourself. Do not post personal information such as your address, phone number, social security number, etc. online. Do not post pictures of yourself online. Make sure you don't put any information online that would enable someone who wanted to harm you to do so. Also remember you cannot control who will see your information once it is online---it could be your mother, a teacher, a prospective employer, or a criminal. Keep this in mind when opening yourself up to others on the internet.

b. Email - It is important to remember that you should never say anything through email that you wouldn't want published in a newspaper. Be careful when responding impulsively to messages. Sometimes when we respond to email or other messages without taking the time to consider our response, we can end up saying things that are hurtful, or threatening. If you write something in

the heat of the moment, it's a good idea to save it in your drafts folder, and reread it before sending it on to make sure that it's really what you mean to say. Never send threatening or offensive email to others, no matter what they may have sent to you. Besides heating up what may already be a tense situation, such messages may in themselves constitute harassment or another crime. Always remember that you are responsible for the content of your email messages and what you say can be used as evidence against you by others.

3.8 Privacy

Elon University will take reasonable efforts to ensure that your user files and email messages remain private, and does not routinely monitor the contents of user files or messages. However, given the nature of computers and electronic communications, we cannot guarantee the absolute privacy of your files and information. You must take reasonable precautions and understand that there is a risk that in some circumstances others can, either intentionally or unintentionally, gain access to files and messages. Where it appears that the integrity, security, or functionality of the University's computer or network resources are at risk or in instances of abuse of University policies, codes, or local, state or federal laws, or when someone's well being is in jeopardy, Elon University reserves the right to take whatever actions it deems necessary (including, but not limited to, monitoring activity and viewing files) to investigate and resolve the situation. The University will treat personal files and communications as confidential, and will only examine or disclose their contents when authorized by the owner or when directed by the combined authorization of the Assistant Vice President of Technology and the appropriate Vice President. Such actions will be taken when there is evidence or reasonable information that inappropriate use of resources is taking place.

Sanctions for inappropriate use of computing, networking and other technology facilities may include, but are not limited to, one or more of the following:

- temporary or permanent revocation of access to some or all computing, networking and other technology facilities?
- disciplinary action according to applicable University policies?
- legal action according to applicable laws and contractual agreements.

Individuals concerned about any violation of this policy are encouraged to contact the Assistant Vice President for Technology or the Vice President for Business, Finance and Technology.