Wells College
Information Technology Policies
Acceptable Use Policy*

(approved August 2, 2017)

Policy Statement

Wells College is committed to academic excellence and providing the resources necessary to maintain academic excellence. Pursuant to this goal, computers, computer accounts, network and Internet access, electronic mail, and related services are provided for use by all members of the College community. Access to and use of the College's computer system is a privilege, and such use must be consistent with the terms of this policy, and with the goals, standards, and overall mission of the College.

Purpose

This policy establishes specific requirements for the use of computing and network resources at Wells College. The College's general policies and codes of conduct apply to the electronic environment just as they apply in all other College settings. This Acceptable Use Policy supplements these existing standards by outlining the special rights and responsibilities that come with using the College's systems, network, and data stores. The College's faculty and staff, are expected to use the computer system only for legitimate purposes consistent with their employment and the College's mission. Students may use the computer system for lawful and proper recreational purposes unless such use interferes with another student's ability to complete their academic work. As with other College policies, violation of the Acceptable Use Policy may result in disciplinary action.

Scope

The Wells College Acceptable Use Policy applies to all staff, students, and faculty of the College. It applies to all systems managed by the Wells College Information Technology Department, and it applies to other systems where the actions of an individual within the Wells College Community is representing the College on other systems or electronic platforms.

Expectations

a) **Abide by the regulations; don't break the law.**
Posting or transmitting any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or material protected by trade secret. Use for product advertisement, political lobbying and activities deemed illegal by law, are strictly prohibited.

b) **Respect intellectual property.**

The use of campus computer resources, including ResNet, to share or distribute copyrighted material to others without the permission of the copyright holder is prohibited. This includes, but is not limited to, using peer-to-peer applications to share these files. 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 potential infringing activity, we will where possible remove or block access to the material in question. Reports of repeated copyright infringements will lead to termination of computer/network services and/or other College/legal actions.

Engaging in copyright infringement or other unauthorized downloading, copying and/or distribution of copyrighted material, violates the U.S. Copyright Act, 17 U.S.C. §§ 101 et. seq. Copyright infringement may subject you to both civil and criminal liabilities. In a civil action, you may be liable for the copyright owner's actual damages plus any profits made from your infringing activity. Alternatively, the copyright owner can elect to recover statutory damages of up to $30,000 or, where the court determines that the infringement was willful, up to $150,000. Copyright infringement may also constitute a federal crime if done willfully and: (1) for purposes of commercial advantage or private financial gain; (2) by the reproduction or distribution, during any 180-day period, of 1 or more copies of 1 or more copyrighted works, which have a total retail value of more than $1,000; or (3) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if you knew or should have known that the work was intended for commercial distribution (17 U.S.C. § 506). Criminal penalties for infringement may include imprisonment for up to 10 years, fines up to $250,000, or both (18 U.S.C. § 2319).

Students who violate the College's policy are also subject to discipline under the College's Student Conduct Code, which may result in sanctions including, but not limited to, written warnings, disciplinary probation, monetary damages and fines, interim suspension, disciplinary suspension and disciplinary expulsion. The sanction imposed for a particular violation will be determined on a case-by-case basis depending on the specific facts and circumstances involved.

c) Access to computer accounts & networks / Non-commercial use only.

Wells College 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 & networks may be unavailable at any particular time.

Wells College reserves the right to restrict or terminate access to its computer and network resources as necessary.

Wells College computer systems and networks are for individual non-commercial use and use related to the educational mission of the College by authorized account holders, and for approved College business activities. Personal use of College IT resources is permitted when it does not interfere with the performance of one's job, or other college responsibilities and does not compromise the functionality or degrade the performance of IT resources, does not consume a significant amount of IT resources, and is otherwise in compliance with this policy. Further limits on personal use by college employees may be imposed in accordance with normal supervisory practices.

Users must respect the finite capacity of the College's IT resources and limit their use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Information Technology Services may set limits on an individual's use of IT resources or require that an individual user refrains from specific uses to assure that these resources can be used by anyone who needs them. Reasonableness of use will be assessed in the context of all relevant circumstances, but any use that degrades the performance of the college network or interferes with the ability of others to use IT resources or with the College's educational or business activities will be considered unacceptable.

d) **Do not install software.**
Only Information Technology staff are to install software or set up web pages or interfaces on any computer or system owned or operated by the College unless approved by and done so in cooperation with IT.

e) **Accounts are for individual use.**
Users may use only those IT resources they are authorized to use, in the manner and to the extent authorized, and they must not attempt to subvert or bypass college-imposed security mechanisms. The use of those credentials is to be used only by the person to whom it has been issued. Users are responsible for all actions originating from their account or network connection. Users must not impersonate others or misrepresent or conceal their identity in electronic messages and actions. Ability to access computers, computer accounts, computer files, or other IT resources does not, by itself, imply authorization to do so.

f) 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: spreading viruses, sending threatening or harassing messages, spamming, packet sniffing, self-perpetuating

programs, excessive volume of file transfers, excessive network traffic. Any action that deliberately or unintentionally degrades or disrupts system or network performance, compromise or circumvents a system or network security, or interferes with the work of others is forbidden.

The use of network hubs, routers, wireless access points, or other devices designed to share your network connection with multiple computers or devices is expressly prohibited.

g) **Respect privacy and security of users and systems.**
Users of the Wells College Network must respect the privacy and security of other users and systems. All information, unless specifically made public and accessible to the end user, should be assumed to be private. If a user discovers the ability, through a loophole, someone's carelessness, etc., to access files, directories, or information that does not belong to them, that information shall be considered private, and the user does not have the right to access it.

All users of the computer system must act responsibly and maintain the integrity of the computer system. The College reserves the right to limit, restrict, revoke, suspend, deny, or extend computing privileges and access to the computer system. Those who do not abide by the College's policies are subject to having: their computer privileges revoked. Including use of and access to the computer system limited, restricted, suspended, revoked, or denied; and may be subject to campus disciplinary procedures, termination of employment, and/or appropriate legal action.

h) **Protect your information**. All users should take steps to avoid phishing scams and other attempts by hackers to steal passwords and sensitive information.

Individuals are required to take reasonable precautions to ensure that their systems are secure -- this includes maintaining current virus detections software at all times on their system(s). Anyone using College resources shall not attempt to access or monitor another user's electronic communications, such as; reading, copying, changing, deleting another user's messages, files, or software, without permission of the user.

i) **Privacy**
Wells College follows industry practices and routinely monitors network traffic to ensure the proper functioning and equitable utilization of the College's computer resources, but by policy does not routinely monitor the contents of user files, messages or network transmissions. 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 College's computers, systems or network resources are at risk the College reserves the right to take whatever actions are necessary to protect its resources. Instances of abuse of College policies, codes, or local, state or federal laws shall be considered risks. Actions may include, but not limited to monitoring activity, scanning specific machines, and viewing files to investigate and resolve the situation.

*This policy replaces in part the previous Computer Internet and Electronic Communications Policy.