STUDENT TECHNOLOGY POLICY

This policy defines the boundaries of "acceptable use" of limited Curtis electronic resources, including computers, networks, e-mail services and electronic information sources. Every student is responsible for using the Curtis Institute of Music (Curtis) electronic mail and Information Technology (IT) systems properly and in accordance with this policy.

A few general items to keep in mind:

• The e-mail and IT systems are the property of Curtis. They have been provided by Curtis for use in your educational life at Curtis.

• The Internet can be a valuable source of information and research. Use of the Internet must be tempered with common sense and good judgment. Use of the Internet via Curtis's computer system constitutes consent by the user to all of the terms and conditions of this policy.

• Electronic devices are often compromised because of the lack of strong passwords. Be sure to create passwords that would be difficult for someone else to guess and do not share them with anyone. Always remember to log out when leaving a website on which you have used a password.

• Electronic devices are valuable tools that are expensive to replace. Please use your good judgment and do not leave your devices unattended. You may wish to purchase insurance coverage for your valuables (see the associate dean of student services for more information).

Copyrighted Material

Downloading and/or sharing copyrighted videos, songs, and other material is illegal. As an artist in training, you should be extra sensitive to the intellectual property rights of others. The e-mail and IT systems of Curtis must not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials. Students may not illegally copy material protected under copyright law or make that material available to others for copying. Students are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material they wish to download or copy. Curtis has installed software designed to block illegal file-sharing, but this software cannot guarantee compliance with the law. Students, if uncertain about whether certain information is copyrighted, proprietary, or otherwise inappropriate for transfer, should resolve all doubts in favor of not transferring the information. The unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject the student to civil, criminal, and institutional liabilities. Illegal peer-to-peer file sharing and/or unauthorized distribution of copyrighted materials using the Curtis information technology system may result in disciplinary action up to and including dismissal from Curtis, as described in the Student Code of Conduct.

All performances sponsored by Curtis either on campus or at other venues are the sole property of Curtis. Students may view these performances for educational purposes only. Students may not use these performances for any other purpose, including posting on social media sites, without the prior written consent of Curtis.

No Expectation of Privacy

The computers and computer accounts given to students are to assist them in their education. Students should not have an expectation of privacy in anything they create, store, send, or receive on the computer network. The computer network consists of Curtis-owned computer work stations, laptops, mobile devices, the wireless network and the infrastructure to support all of the above, as well as all network traffic.

Remember, you are accountable for what you and your computer and/or mobile devices do on the network, whether it is intentional or not.

Disclaimer of Liability for Use of Internet
The Internet is a worldwide network of computers that contains billions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. It can be difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail and electronic messages containing offensive content. Users accessing the Internet do so at their own risk.

Blocking of Inappropriate Content
Because we are governed by Federal Trade Commission (FTC) regulations, we have software that is designed to prevent our system from being subject to unauthorized activity. Inappropriate sites may be blocked from access by Curtis. In the event you encounter inappropriate material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to our internal blocking software. If you are trying to download material you feel is safe but is being blocked, please contact the appropriate staff person for assistance.

Accessing the Internet
To ensure security and to avoid the spread of viruses, students accessing the Internet through a computer attached to Curtis's network must do so through an approved Internet firewall. Accessing the Internet directly from separate Internet connections not maintained by Curtis, e.g., non-Curtis WiFi or cellphone modem is strictly prohibited unless the computer you are using is not connected to the Curtis network. Students are not permitted to setup their own wireless networks anywhere at Curtis.

Duty to Not Waste Computer Resources
Students must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet in our labs or public access areas (for example, the Student Lounges, Rock Resource Center, Lenfest Hall computer lab, etc.), playing games when other students need to use the computer for school work, engaging in online chat groups that monopolize the computer, printing multiple copies of documents, or otherwise creating unnecessary network traffic. Because audio, video, and picture files can require significant storage space and/or bandwidth, files of this or any other sort should not be downloaded unless they are related to your education.

All e-mail and electronic messages are stored on a central backup system in the normal course of data management.

Your email account has a limited amount of storage space. Users should routinely delete outdated or otherwise unnecessary e-mail and computer files. Electronic housekeeping will keep the system running smoothly and effectively, as well as minimize maintenance.

Students are reminded to be courteous to other users of the system and always to conduct themselves in a professional manner. Electronic messages are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient. Remember the golden rule of computing: Would you want your e-mail message, text, or Facebook comment to appear on the front page of the New York Times?

Prohibited Activities

The following activities are not permitted:

• Engaging in the unauthorized entry into or transfer of any Curtis computer file or the file or computer of any member of the Curtis community.

• Using or attempting to use another person's identification or password or computer account.

• Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication.

• The interception or attempted interception of communications by parties not explicitly intended to receive them.

• Making Curtis computer facilities or resources available to individuals not affiliated with Curtis without approval by an authorized Curtis official.

• Alteration of the content of a message originating from another person or computer with intent to deceive.

• Use of any computer or electronic device to interfere with the work of another member of the community and/or the normal operation of Curtis.

• Use of Curtis computers, e-mail accounts, or labs for illegal purposes or for the transmission of material that is unlawful, harassing, libelous, invasive of another's privacy, abusive, threatening, harmful, vulgar, obscene, or otherwise objectionable, or that infringes or may infringe upon the intellectual property or other rights of a person or organization. This applies to the use of electronic messaging, texting, Facebook or any other social media outlet.

• Cyber-bullying.

• Engaging in harassment (sexual or other) through e-mail, social media or other IT systems. No e-mail or other electronic message should be created or sent if it contains intimidating, hostile, or offensive material concerning race, color, religion, sex, age, national origin, disability, or any other classification protected by law.

• Intentionally compromising the privacy or security of electronic information, including changing the configuration of the computers established by Curtis and its IT consultants, including altering a computer to a non-English language format.

• Soliciting for religious or political causes, commercial enterprises, pyramid schemes, outside organizations, or other non-educational or non-professional-related purposes.

Violation of any of these regulations may result in your loss of computing privileges and/or disciplinary action under the Lenfest Hall Housing Agreement or the Student Code of Conduct.

Virus Detection

Files obtained from sources outside Curtis, including storage devices brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail; and files provided by customers or vendors may contain dangerous computer viruses that may

damage Curtis's computer network. Students should never download files from the Internet, open e-mail and attachments from outsiders, or use storage devices from non-Curtis sources without first scanning the material with virus-checking software. If you suspect that a virus has been introduced into the Curtis's network, notify the associate dean of student and academic affairs immediately.

Information Security Education, Training, and Threat Awareness
Compliance with the Policy is the responsibility of every member of the Curtis community, including students, faculty, staff, and contractors. Information security training and awareness is a significant part of an effective computer security strategy.

Accordingly, Curtis's Information Technology Department communicates security threats to members of its community in several ways, including email messages and postings to the main page of the Curtis Portal. Our partners at IT Services, a contracted agency the provides significant network support to Curtis, also use email to communicate about computer security issues. Every member of the Curtis community is responsible for paying close attention to, and acting upon these notices.

Curtis's IT Department occasionally schedules talks and training on computer security-related issues. These sessions cover computer security on campus, as well as important topics that are valuable to security outside school as well. We encourage participation in these events by all members of the Curtis community.

Anyone who notices unusual and/or suspicious activity while logged into Curtis's network, clicks on a suspicious link, or suspects that a device is compromised should report these issues to infotech@curtis.edu or speak to an IT Department representative.