STUDENT INFORMATION TECHNOLOGY POLICY

Policy Title	Information Technology & Systems Support and Usage Student Policy
Policy Owner	Senior Director of Academic and Information Technology
Date	August 2025

Section 1 Scope and Purpose

This policy must be followed in conjunction with other policies of the Curtis Institute of Music ("Curtis") governing appropriate conduct and behavior. The Curtis Institute of Music complies with all applicable federal, state, and local laws and nothing contained herein should be construed to violate any of the rights or responsibilities contained in such laws.

Security is everyone's responsibility. Our students, faculty, staff, board, patrons, and donors are the life blood of our organization. Protecting their personal and confidential information must be of the utmost concern for every member of our Curtis community. The following policy is designed to outline the minimum steps each student is expected to take to help maintain our technological security. This policy is neither exclusive nor all-inclusive as technology changes rapidly. Each student is charged with using their best judgment when using Curtis's hardware and applications and accessing Curtis systems and data.

If you have questions regarding the appropriate use of Curtis electronics, communications equipment, systems, software, applications, or technology, including e-mail and the Internet, please contact your supervisor, manager, or the IT department.

Section 2 Computer, Phone, Printer, and other Usage

1. All technology provided by Curtis, including computer systems, communications networks, related work records, and other information stored electronically, is the property of Curtis. In general, use of Curtis technology systems and electronic communications should be for educational purposes only. Students receiving Curtis's devices will sign a Mobile Device Policy which clearly defines how Curtis owned property should be used.

Section 3 Internet and Email

1. Curtis Institute of Music recognizes that use of the Internet and e-mail has many benefits and can make student communication more efficient and effective. However, students are expected to use the Internet and e-mail systems appropriately.

2. Students may not use Curtis Institute of Music's Internet, e-mail, or other electronic communications to transmit, retrieve, or store any communications or other content of a defamatory, discriminatory, harassing, or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference may be transmitted. Harassment of any kind is prohibited. Disparaging, abusive, profane, or offensive language, materials that might adversely or negatively reflect on Curtis or be contrary to its legitimate business interests, any illegal activities, including, without limitation, piracy, cracking, extortion, blackmail, copyright infringement, and unauthorized access to any computers on the Internet or e-mail are forbidden. Use of Curtis computers for any unapproved activity may be traced to the registered IP addresses.

3. Students are personally responsible for the content they publish on blogs, social media sites, or any other form of user-generated media, whether it is

sent from Curtis Institute of Music controlled hardware or software. Disrespectful and offensive posts, including inappropriate or degrading remarks about Curtis, its students, or its employees, will have the same disciplinary result as if those remarks were made in person at the organization.

4. Every student of Curtis is responsible for the content of all text, audio, or image files that he or she places or sends over Curtis's Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. Curtis's corporate identity is attached to all outgoing e-mail communications, which should reflect Curtis values and appropriate language and conduct.

5. Students must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials, except with written permission or as a single copy for reference only. Sharing the URL (uniform resource locator or "address") of an Internet site with other interested persons for business reasons is permitted.

6. Students may not use the system in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and "spamming" (sending e-mail to thousands of users) except as pre-approved mass communication.

7. E-mail and other electronic communications transmitted by Curtis equipment, systems and networks are neither private nor confidential. All such transmissions are the property of Curtis.

8. To help reduce organizational hosting and labor costs, the following policy will be applied to all graduating students. Accounts will be converted to

alumni.curtis.edu accounts upon graduation. If you do not access your alumni account at least once a year, it will be disabled.

Section 4 Sensitive Information and Passwords

1. Sensitive information is any information that could be used by criminals to conduct identity theft, blackmail, stalking, or other crimes against an individual. This includes your sensitive personal information, the information of the board, donors and patrons, activity participants, students, and the public at large. The Curtis Institute of Music requires that all State and Federal laws and regulations be followed in addition to all requirements of this policy.

   Sensitive information includes, according to the Department of Homeland Security, but is not limited to following:

   - Social security numbers and alien registration numbers,
   - Bank account numbers,
   - Passport information,
   - Healthcare-related information,
   - Medical insurance information,
   - Credit and debit card numbers,
   - Driver's license and State ID information,
   - Racial or ethnic origin,
   - Political opinions,
   - Religious or other similar beliefs,
   - Membership of trade unions,
   - Physical or mental health or condition,
   - Sexual orientation and/or activities,
   - Full date of birth, and

- Authentication information such as mother's maiden name or passwords.

2. Never leave sensitive information in hard copy (on paper, note cards, etc.) unattended and unsecure, such as on a desk, network printer, fax machine, or copier. Secure such information, in a locked drawer, cabinet, desk, or safe, when not in use or not otherwise under your control.

3. Do not send sensitive information unprotected. If possible, scan and then encrypt or password protect the document(s). If the attachment is password protected, provide the password separately (e.g., by phone, another email, or in person).

4. Avoid discussing sensitive information in person or over the telephone when you are within earshot of anyone unauthorized to possess the information. If you must discuss sensitive information using a speakerphone, phone bridge or video teleconference, do so only if you are in a location where those unauthorized cannot overhear. Keep in mind that phone conversations are easily overheard between workstations. Sensitive information is most securely discussed in an office, conference room, or behind a closed door.

5. Passwords must not be shared with anyone. All passwords are to be treated as confidential information.

    - Do not insert passwords into email messages or other forms of electronic communication.
    - Do not reveal passwords over the phone to anyone.
    - Do not reveal a password on questionnaires or security forms.
    - Do not hint at the format of a password (for example, "my family name").
    - Do not share Curtis Institute of Music passwords with anyone.
    - Do not write passwords down and store them anywhere near your equipment.

- Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers). Instead use a password management tool (LastPass, Keychain)
- Do not use the same password for Curtis Institute of Music accounts as for other non-Curtis Institute of Music access (for example, personal email accounts, social media accounts, gaming console accounts, etc.)

6. Any user suspecting that student passwords may have been compromised must report the incident to IT and change all passwords. IT team or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it. Under no circumstances may an individual, department, or outside group perform such scans. Such actions would be considered a cyber-attack against Curtis and dealt with accordingly.

Section 5 Acceptable Use

1. Personal devices may not be used at any time to:

    - Store or transmit proprietary information belonging to either Curtis, one of its employees, directors, or any another business without written prior permission.
    - Store or transmit illicit materials.

2. All computers (including personally owned) connecting to the network, whether through hardline or wireless connection, VPN, or wireless are required to install and enable anti-virus software. Installation, troubleshooting, and maintenance of the anti-virus software are the

responsibility of all utilizing personal computers or other BYOD devices connecting to the network. IT may require proof or validation of such anti-virus software being present on a device before permitting access to any Curtis Institute of Music network or application. Failure to demonstrate sufficient anti-virus protection may result in the device being disallowed from accessing an application, a particular network (such as guest only, no wireless access), or any access to Curtis systems.

3. This policy does not preclude IT from implementing a more stringent requirement.

4. Curtis reserves the right to disconnect devices or disable services without notification. The student is expected to always use their devices in an ethical manner and adhere to the Curtis Institute of Music's acceptable use policy as outlined above.

Section 6 Loss, Right to Monitor, and Consequences of Violations

1. Lost or stolen devices, whether personal or Curtis Institute of Music owned, must be reported to the IT Department within 24 hours. This applies to all types of devices able to access Curtis's network or other Curtis data such as email and OneDrive data.

2. All Curtis-supplied technology, including computer systems, equipment, and Curtis Institute of Music-related work records, belong to The Curtis Institute of Music and not to the user.

3. Curtis routinely monitors network traffic patterns, and students should observe appropriate discretion in their use and maintenance of such Curtis property.

4. E-mail and other electronic communications transmitted by Curtis's equipment, systems and networks are not private or confidential, and they are the property of Curtis. Therefore, Curtis reserves the right to examine, monitor and regulate e-mail and other electronic communications, files, and all other content, including Internet use, transmitted by, or stored in its technology systems, whether onsite or offsite. Monitoring may occur during litigation, for audit related purposes, or for a cybersecurity or personnel investigation. All monitoring would be approved by the appropriate parties.

5. Because all the computer systems and software, including e-mail and Internet connections, are the property of Curtis, all policies apply to their use and are always in effect. Violations of the word or spirit of any part of this policy will be reviewed on a case-by-case basis. Consequences include, but are not limited to, revocation of privilege of use or access to Curtis equipment, networks, applications, and individual disciplinary actions. Additionally, by failing to follow any of these provisions, students assume full liability for risks including, but not limited to, the partial or complete loss of Curtis and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render a device unusable.

6. Any student who abuses Curtis-provided access to e-mail, the Internet, or other electronic communications or networks, including social media, may be denied future access, and, if appropriate, be subject to disciplinary action in accordance with this policy. Consequences of violating the anti-virus provision include the computer being blocked from the network in addition to the other potential disciplinary measures in this policy. Computers will not be unblocked until the machine is cleaned and brought into compliance.

Section 7 Best Practices for Social Media for Curtis Employees & Students

This section is meant as a set of recommendations or best practices for social media use to help you maintain a professional online profile.

Do

- Be respectful and positive. Respect the views of others, even if you disagree. Remember, many different audiences view your posts including potential students, audiences, donors, alumni, children, parents, faculty, etc. Take the high ground. If you identify your affiliation with Curtis in your comments, readers will associate you with the school, even with the disclaimer that your views are your own.
- Be responsible. Think twice before posting. If you wouldn't want your colleagues, parents, or a future employer to see your post, don't post it.
- Think ahead. The internet is permanent. Even if you delete something, it's still out there somewhere. Potential employers sometimes use these social media websites to screen candidates.
- Remain transparent. If you choose to promote Curtis, please identify yourself as a Curtis employee or student. Don't hide your identity for the purpose of promoting Curtis through social media.
- Protect others. Do not share personally identifiable information about other students, faculty, alumni, or staff without permission.
- Protect yourself. While you want to be honest about yourself, don't provide personal information that scam artists or identity thieves could use against you. Don't list your home address, telephone number, or email address. Be aware of "phishers" or those who might try to hack your account and reset your password in the event of a breach. Always log out of your account when using public computers.

- Link back. You are welcome to link from your social media site to the Curtis homepage and Curtis social media sites.
- Follow the rules. Remember that laws and Curtis' policies governing inappropriate conduct such as sexual (or other) harassment, bullying, discrimination, defamation, infringement of copyright and trademark rights, and unauthorized disclosure of student records and other confidential and private information apply to communications by Curtis students, faculty, and staff through social media. Obey the Terms of Service of any social media site or platform on which you participate. Violation of the Student Code of Conduct, the terms of the staff and faculty handbooks, or Curtis' employment policies may result in disciplinary action.

Do Not

- Do not use Curtis' logos without approval. Additionally, do not create or develop social media accounts, profiles or initiatives bearing Curtis' name without prior approval. Social media accounts, profiles, and initiatives must be approved by the communications and marketing departments.
- Do not modify or use the Curtis logo or name for personal endorsements or to promote a product, cause, political party, or candidate.
- Do not represent your personal opinions as endorsed by Curtis.
- Do not establish an email account using the Curtis name without authorization. E.g., curtisatheleticdepartment@gmail.com.