CLEVELAND INSTITUTE OF MUSIC

CIM Acceptable Use of Technology Policy

revised 01/07/16

Introduction

The Cleveland Institute of Music (CIM) provides information technology systems to support the mission of the Institute. The use of CIM information technology systems, including its computer systems, networks and the data contained therein, is governed by a set of rules contained in this Acceptable Use of Technology Policy.

Users of CIM information technology systems are subject to this policy and are expected to read, understand, and comply fully with its provisions. Users found in violation are subject to disciplinary action, including temporary or permanent denial of access to information technology systems, separation or termination from the Institute. Violators may also be subject to action by campus, civil, or criminal judicial systems. This policy is subject to change at any time. The most current policy can always be found on our website, www.cim.edu.

CIM provides Internet access via a high speed fiber-optic network and wireless networking connected to the Case Western Reserve University network. CIM offers wired connections to the Case network for personal laptops in the Robinson Music Library. Residents of our dormitory will also find each room contains a wired connection to the Case network for their personal computer there. Wireless connections to the Case network are offered at various locations throughout CIM. The Technology Learning Center (TLC) has computers connected to the Case network for Conservatory students, faculty and staff use. Therefore, users of network technology resources are also bound by the Case Technology Acceptable Use Policy, which can be found at http://www.case.edu/its/security/docs/aup.htm.

Institutional Privileges

CIM provides information technology systems for CIM use only and we reserve the right to monitor and log usage data. Collected data includes contents of communications and data transmitted over, or stored in, information technology systems. All data created on, stored on or transmitted on technology information systems are CIM records. CIM has the right, but not the duty, to monitor any and all aspects of the information technology systems, including, but not limited to, monitoring sites visited on the Internet, monitoring chat and newsgroups, reviewing material downloaded or uploaded by users, and reviewing e-mail messages sent and received. We may monitor our computers to determine compliance with CIM policies, to investigate possible misconduct, to locate information, or for any other purpose.

By using CIM information technology systems, you waive any right to privacy in anything you create, store, send or receive on the computer or the Internet. CIM may suspend privileges of an individual user for reasons relating to physical or emotional safety and well being, or for reasons relating to the safety and well being of other members of the CIM community or CIM property.

CIM does not and will not act as a censor of information, but will investigate properly identified allegations arising from the CIM community and will comply with applicable state and federal laws. CIM will fully comply with the authorities to provide any information necessary for the litigation process and will report criminal offenses to the appropriate authorities.

Security and Network

Access to server rooms is restricted to members of the CIM IT Department. No individuals are allowed in a server room unless they are under immediate supervision of an authorized CIM IT staff member.

Tampering with equipment is prohibited. You may not cause intentional destruction or damage to equipment, software, or data.

Connection of a non-CIM owned computing device to the CIM network is prohibited. Users may not alter the CIM network infrastructure by installing any unauthorized networking equipment including, but not limited to, hubs, switches, routers, or wireless access points of any kind. It is a violation to install any devices or drivers on CIM owned computers. It is also a violation to connect devices to the CIM network that are designed to alter, reshape, affect, monitor, or intercept network traffic.

Only CIM IT staff may install or uninstall devices or software on CIM owned computers. All software in use on CIM computers is officially licensed software. No software may be loaded, installed or used, by any means of transmission other than software provided by CIM IT Department. In addition, you may not download or install software obtained from the Internet or from computers or networks that do not belong to CIM, even though indications are the software may be “free.” Downloading of software is prohibited.

You may only access the Internet through an approved Internet firewall. Accessing the Internet by other means is prohibited unless the accessing computer is not connected to the CIM network. No user may cancel or modify security measures on a CIM computer setup by the CIM IT Department, such as stopping virus scans or Windows updates. Computers must be logged off to a point that requires a new logon or locked whenever you leave the work area. All technology equipment in your office is to be powered off overnight. Computers should be shutdown, which will automatically power them off. Printers, scanners and other devices will need to be shut off with the power button. Do not unplug devices or power them off using electrical cords. Movement of any technology equipment or any modifications that require unplugging of cords should be done by CIM IT staff only.

Any user who finds a violation or possible security lapse on a CIM system is obligated to immediately report it to the CIM IT Department. Loopholes in system security are not to be used to damage systems or obtain unauthorized access. All technology issues for CIM information systems should be reported to the CIM help desk at extension 367 or help@cim.edu. CIM reserves the right to terminate or limit the network connectivity of any user whose online activities are deemed detrimental to the health of the network.

User Accounts

Members of the CIM community are provided with accounts and passwords to access information systems. Access to information technology systems is based on the need to use specific data, as defined by role or position, and will be annually re-evaluated. The person holding an account is responsible for its use, and all activity originating from that account, at all times. Account holders are expected to protect passwords and keep them confidential. Sharing of accounts or passwords is prohibited. Passwords should be changed frequently. Any attempt to gain access to an account or determine the passwords of other users is strictly prohibited. Where possible, systems lock out a user after 5 unsuccessful attempts to log on. Locked out users can only be unlocked by the CIM IT Department.

Systems accounts are owned by CIM and are to be used for CIM-related activities only. A user must identify themselves, by showing a CIM ID card, to any CIM staff member or student employee who requests verification. Accounts remain in effect as long as the user maintains an official relationship with CIM. Accounts are created or deleted upon notification to the CIM IT staff from the Registrar or Human Resources Department. Administrators of CIM information systems, other than systems supplied by CIM IT, must file passwords for those systems with the CIM IT Department.

Members of the CIM community are expected to safeguard the integrity, accuracy and confidentially of data on information technology systems. You may not use CIM information technology systems for storing, transmitting, or receiving any information that may be seen by others as discriminatory or harassing. Users must not use any communications services to intimidate, insult, or harass others. Downloading onto your desktop or transmitting any inappropriate images, photos, sounds, email attachments or messages is prohibited. You may not use CIM information technology systems to solicit others for commercial ventures, religious or personal causes, outside organizations, broadcasting unsolicited messages or other similar, non-CIM related matters. No user account may be used for unethical, illegal, or criminal purposes. Accessing files or directories of other users is not permitted. Unauthorized monitoring of electronic communications is prohibited.

Users must abide by all applicable copyright laws and licenses. Users are also responsible for assisting in the protection of the systems they use. You are not allowed to copy programs, take them home, distribute, or sell them to others. You are not allowed to use CIM resources to obtain or to print copyrighted materials.

Individual Privileges

Users must respect the privacy and personal rights of others. Computer programs, email, voice mail and electronic files can only be accessed by authorized personnel for compelling business or security reasons. Information that users obtain through special privileges is will be respected under Personal Privacy Information (PPI) guidelines. User privacy cannot be extended under conditions such as a program causing disruption to the network or other shared resources or the suspected violation of CIM policy, state or federal law.

While some incidental personal use of CIM computing resources may be allowed, it is not appropriate for users to convert CIM resources to private endeavors. All personal communications and stored data will be treated the same as other communications and data. We may access and disclose, in accordance to this policy, all communications and data within CIM information technology systems, without regard to content. No information technology system may be used for improper purposes, such as computer games, gambling or the playing of practical jokes.

You may not download any confidential or proprietary files or documents to your remote computer. If you must work on these materials from a remote location, you must use the computer network without transferring the file or document to your remote location.

Violations of this policy will be governed under the disciplinary procedures as stated in the faculty, staff or student handbook, whichever is applicable. For questions or clarification on this policy, please contact Daniel Betting, Director of Information Technology at Daniel.Betting@cim.edu.