Cleveland Institute of Art

Acceptable Use Policy

Cleveland Institute of Art (CIA) makes available to authorized users computer facilities and services to support its mission of providing an environment which encourages innovative teaching, learning, and research.

Authorized Use

An authorized user is any person granted authority by the Institute to access its computing and network systems and whose usage of these resources complies with this policy. Unauthorized use is strictly prohibited.

Rights and Responsibilities

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Personal responsibility assumes that each user shall:

- Protect his/her passwords
- Report any observed or attempted breach of security by others
- Change his/her password as required or requested
- Participate in cybersecurity training as required by Information Technology
- **Make frequent and appropriate backups of their own work to guarantee protection against loss**
- Clearly label personal works and opinions as his/her own before they are distributed to others
- Respect the rights of others, the integrity of the systems, and related physical resources
- Abide by applicable state and federal legislation
- Respect the confidentiality of records

Existing Legal Context and Enforcement

All existing local, state, and federal laws; license agreements; and all Institute regulations and policies apply.

Complaints alleging misuse of campus computing and network resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

Misuse of computing, networking, or information resources may result in the restriction or discontinuation of computing privileges and may be prosecuted under applicable statutes. Further, users are accountable for following Institute policies and procedures. Those found in violation are subject to a full range of

sanctions including, but not limited to, the loss of computer or network access privileges, disciplinary action, and dismissal from the Institute. Some violations of this policy may constitute criminal offenses, as defined by local, state, and federal laws and the Institute may, at its option, prosecute any such violations to the full extent of the law.

Students and employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files as required to protect the integrity of computer systems.

Authority

While respecting the individual's right to privacy, the Institute and the Information Technology staff reserves the right to access the files of others for the maintenance of its computer, network and storage resources and to monitor the use of these resources for excessive or inappropriate use.

Examples of Misuse

Examples of misuse include, but are not limited to, the activities in the following list.

- Using a computer account that you are not authorized to use
- Obtaining a password for a computer account without the consent of the account owner.
- Using the Institute network to gain unauthorized access to any computer systems
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms
- Attempting to circumvent data protection schemes or uncover security loopholes
- Violating terms of applicable software licensing agreements or copyright laws
- Deliberately wasting computing resources
- Using electronic mail and/or other computer applications to harass or intimidate others
- Using electronic mail and/or other computer applications to disrupt the activities or safety of others
- Using electronic mail to send mass mailing without prior administrative and IT authorization
- Masking the identity of an account or machine
- Posting materials on electronic bulletin boards that violate existing laws or the Institutes codes of conduct
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Use of Institute computing facilities and resources for private business, commercial or political activities, fundraising, advertising on behalf of non-CIA organizations, unlawful activities or uses that violate other Institute policies
- Installation or running of any Institute-unauthorized software, including mobile code technologies

Activities will not be considered misuse when authorized by appropriate Institute officials for security or performance testing.

Data Protection

Confidential Institute information must be maintained in the safest environment possible consistent with teaching, learning, operations and research needs. CIA employs the principle of least privilege in which a user is given the minimum levels of access needed to perform their job duty. While Information Technology audits user accounts on a quarterly basis, supervisors should proactively work with Information Technology to ensure that authorizations for confidential information are up-to-date as employees are hired, change roles or separate from the Institute.

Passwords and Authentication

Access to electronic information must be protected by strong passwords. Passwords must never be shared with anyone. Passwords should be changed as best practice, or individual system policies. Multi-factor authentication (MFA) may be required for many Institute systems. When using MFA, authenticator app use is preferred over SMS.

Endpoint Protection

CIA supports and maintains endpoint protection for all Institute-owned laptops and desktops.

Personally Owned Devices

Use a properly secured device to gain remote access to CIA networks and systems. Do not use devices shared with others for accessing confidential Institute information. Avoid downloading confidential information to personal devices and avoid transmitting sensitive data by forwarding via email.

If you use a mobile device to access Institute data, the device must be properly secured with a passcode or biometric access control and with encryption.

Employees and students are responsible for applying recommended security updates and patches on a timely basis on their personal devices that connect to CIA networks and systems. They must install updates or patches that vendors identify as critical as soon as reasonably possible after release.

Employees must ensure they are using current endpoint protection on any device they use for CIA business.

In the event that employees or students do not have access to a properly secured device, a limited number of laptops are available for temporary use in the Equipment Checkout (Room 325).

Secure Data Deletion

Information no longer needed for teaching, learning, operations and research needs and not necessary to retain by law or Institute policy must be securely deleted as a regular business process or once discovered.

Enforcement

This policy will be enforced by the Associate Vice President of Information Services and Technology, Associate Director of Network Administration, and CIA Administration. Violations of this policy may result in disciplinary actions, up to and including termination. Where illegal activities or theft of CIA property

(physical or intellectual) are suspected, CIA Administration may report these activities to applicable authorities.