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. This policy covers authorized use, rights and responsibilities, data protection, the use of artificial intelligence for administrative purposes by CIA employees, and software and online services use by CIA employees.

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.

Edited 3-19-24

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.

Policy for Responsible Administrative Use of Generative AI Online Services at CIA for CIA Employees

Introduction: CIA employees are expected to exercise caution and discretion when using confidential data with generative artificial intelligence online services, such as chatbots or text generators, for educational, productivity, or general purposes. Generative AI services may have the potential to store, analyze, or inadvertently expose data inputted by users, which can include raw text, images, audio, or video. Therefore, the following policy must be adhered to:

1. Before using any confidential institutional data with an AI service, CIA employees should get approval from Information Technology by submitting a support ticket at support.cia.edu.

2. Protecting Institutional Information

a. Definition of Confidential Data: Within the context of our institution, confidential data encompasses any non-public, sensitive, and private information. This includes, but is not limited to:

- Personal details of students, faculty, and staff (addresses, phone numbers, social security numbers, financial data, academic records).
- Information about patrons, donors, or alumni.
- Health and medical records of any individual associated with the institution.
- Institution-specific business plans, strategies, and internal communications.
- Financial data and budgets.
- Intellectual property, including proprietary designs, methodologies, and copyrighted content.
- Proprietary research, curricula, and academic papers.

b. Interaction with AI Services: Ensure that no confidential data, as defined above, is inputted, uploaded, or otherwise exposed to the AI service. Instead, users should always generalize, anonymize, or omit sensitive details when querying or interacting with the service.

3. Safeguarding Login Credentials

a. Protect User Credentials: User credentials, including usernames, passwords, PINs, recovery phrases, or any other access-related data, must never be shared or included in prompts or inputs for generative AI services.

b. Credential Safety Training: Users should undergo training on the importance of maintaining the secrecy of login credentials and the risks associated with unintentional exposure. (KnowB4)

4. Assume Accessibility

a. Data Accessibility Awareness: Be aware that any content shared, even inadvertently, with generative AI services might be accessible by others.

b. Exercise Prudence: Maintain a vigilant and cautious approach in interactions with AI services. Avoid sharing or discussing any information that could compromise personal or institutional data security.

Online Services/Software Request Policy and Procedures For CIA Employees

1. Online Service Acquisition Policy:

Online Service Definition:

An online service (free and paid) is any tool or service accessed from the internet through a web browser or browser-based application. A CIA online service provides functionality to accomplish work performed in the service of the Cleveland Institute of Art.

Services that require software installation are covered under the Software policy (see section 2).

The Online Services Department acts as a support and usage consultant for the many online or web-based tools available to CIA faculty, staff, and students.

A function of the Online Services Department is to have awareness and administrative access to all official online services at CIA. Online Services may play various roles related to the services, based on how the service is used by CIA. This access is not to be interpreted as ownership, or as having managerial or financial responsibility for a specific service. At the bare minimum, administrative access provides a “break glass” emergency solution—similar to the cabinet of keys of a facilities manager.

Any online service required for CIA employees or students to perform their work must be approved by the Associate Director of Online Services (ADOS) or the Associate Vice President of Information Systems + Technology. This approval may be requested by logging a support ticket at support.cia.edu.

The ADOS must be provided administrative access to all approved and supported Online Services.

Neither Online Services, nor any IT staff will be expected or required to support unapproved online services. Existing online service accounts that were in place prior to publication of this policy must be reported to the ADOS. Administrative access must also be granted to the ADOS. Administrative account access does not imply ownership of related processes or content used in connection with the service.

No account should be created using a non-CIA provided email address. Existing service accounts must be converted to use a CIA email address.

Services will be assessed based on current applicable security, financial, and accessibility standards.
The request process will include:

- Review of requirements
- Review of current services
- Assessment of service related to current applicable cybersecurity, financial, and accessibility standards (see section 5)
- Decision to adopt the new service or an existing CIA service

The process may be as informal or formal as the project dictates. Written communication should be utilized at all stages to preserve a history of decision making.

Denial of approval for an online service does not remove said service from future consideration.

2. Software Acquisition Policy:

Software Definition:

Applications (free and paid) that require local installation on a laptop, desktop, or server are considered Software. Services with the primary functionality accessed through a browser, but also offers the option of software or mobile app installation, are considered online services (see section 1).

Any software required for CIA employees and students to perform their work must be approved by the respective Faculty Chair, Manager of Technical Services or the Associate Vice President of Information Systems + Technology. This approval may be requested by logging a support ticket at support.cia.edu.

IT staff will not be expected or required to support unapproved software. Unapproved software will be removed from CIA devices upon discovery.

Software required to be installed in computer labs must be requested and approved prior to July 1st to guarantee that the software will be ready to use by the start of classes in the Fall Semester. IT staff will make reasonable accommodations to install/update lab software throughout the academic year. These requests will be handled on an ad hoc basis by the Manager of Technical Services.

Software will be assessed based on current applicable security, financial, and accessibility standards.
The request process will include

- Review of requirements
- Review of currently owned software
- Assessment of software related to current applicable cybersecurity, financial, and accessibility standards (see section 5)
- Decision to adopt the new service or an existing CIA software

The process may be as informal or formal as the project dictates. Written communication should be utilized at all stages to preserve a history of decision making.

Denial for software does not remove said software from future consideration.

3.Online Services and Software Request Process

It is recommended that a faculty/staff member involves a member of Information Technology during department or committee preliminary needs discussions, before selecting an online service or software application. Requests for consultation can be submitted in a support ticket at support.cia.edu.

Trial accounts or demo software may need to be created to facilitate the assessment of a software/service functionality. Trial accounts or demo software should only be used in consultation with IT staff.

4. Payment and account management

Online services and software serving more than one department will be included in the Online Services or Technical Services budget, provided that these services have been approved as a part of the CIA budget process. The budget source for first-year account activation payments will be determined at the time of the approval and account creation. CIA reserves the right to deny reimbursement for unapproved online services and software.

5. Online Service/Software Assessment Criteria

Assessment of Online Services and Software includes the following:

- Non-profit/EDU pricing
- Team management
- License management
- WCAG (current recommended level) compliance
- Cybersecurity via completed HECVAT form
- Does it duplicate functionality already offered in a current CIA Online Service or Software?
- What existing process does it serve?
- Will it replace a service/software or add to the list of services/software?
- Is Data migration expected or required?
- Data processing
- Payment processing
- What process does it support and who is the process owner?
- Is the requesting party the process owner or a representative?

6. Online Service/Software Approval, Account Creation and Installation

The ADOS will work directly with the requesting party to create the newly approved service account.

The Manager of Technical Services will work directly with the requestor to install the software.