



THE COOPER UNION  
FOR THE ADVANCEMENT  
OF SCIENCE AND ART  
**INFORMATION TECHNOLOGY  
ACCEPTABLE USE POLICY**

APPROVED JULY 17, 2026



# APPROPRIATE USE OF COOPER UNION INFORMATION TECHNOLOGY SYSTEMS

## SCOPE AND PURPOSE

This policy applies to all Users of Information Technology (“IT”) Systems, owned or licensed by the Cooper Union for the Advancement of Science and Art (the “Cooper Union” or “College”) including but not limited to Cooper Union students, faculty, and staff, external contractors, and guests. Cooper Union IT Systems include and are not limited to hardware, software, networks, networked shared drives, file servers, and any secure facilities administered by the Cooper Union IT Department, as well as private machines and systems administered by individual schools, departments, and laboratories within Cooper Union that share Cooper Union’s network and IT resources.

## RISK & COMPLIANCE ALIGNMENT

This policy supports Cooper Union’s information security and privacy program and aligns with applicable standards and regulations, including but not limited to FERPA, applicable state privacy laws, contractual requirements, and recognized cybersecurity best practices such as the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 principles.

## POLICY STATEMENT

Information technology (“IT”) is used daily to create, access, examine, store, and distribute documents, files, and multiple media and formats. Information technology plays an integral part in the fulfillment of Cooper Union’s educational, administrative, and other roles. Users of Cooper Union’s IT resources are responsible for their proper use. The policies of Cooper Union’s Information Technology Department govern the use of Cooper Union IT Systems.

The purpose of this policy is to ensure information technology standards that promote Cooper Union’s missions in teaching, learning, research, administration, and public discourse. This policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and most effective performance of IT Systems;
- To ensure that the use of IT Systems is consistent with the principles and values that govern the use of Cooper Union facilities and services;
- To ensure that IT systems are used for their intended purposes, and that use of IT systems is lawful, ethical, responsible, and in accordance with all Cooper Union policies, including safeguarding institutional data; and
- To establish clear processes for addressing policy violations.

## DEFINITIONS

**IT Systems:** These are servers, personal computing devices, applications, printers, networks (virtual, wired, and wireless), online and offline storage media, and related equipment, software, and data files that are owned, managed, or maintained by Cooper Union. For example, IT Systems include institutional and departmental information systems, faculty research systems, computer workstations and laptops, the College's campus network, computer labs, and computer clusters.

**User:** A "User" is any person, whether authorized or not, who makes use of any Cooper Union IT System from any location.

**Systems Authority:** While Cooper Union is the legal owner or operator of all IT Systems, it delegates oversight of systems to the specific department head or administrative office of Cooper Union ("Systems Authority") and Information Technology Department.

**System Administrator:** System Administrators oversee the day-to-day operations of IT Systems and are authorized to determine who is permitted access to IT Systems.

**Specific Authorization:** This means documented permission provided by the applicable Systems Authority.

# POLICY STATEMENT AND PROCEDURES

## APPROPRIATE USE OF IT SYSTEMS

This Policy sets forth the general parameters of the appropriate use of IT Systems for all users, including the policy for onboarding, transfer, and termination.

### APPROPRIATE USE

IT Systems may be used only for their authorized purposes – that is, to support the research, education, administrative, and other functions of Cooper Union. The purposes of any IT System and the nature and scope of authorized, incidental personal use may vary according to the User's duties and responsibilities. Appropriate use restrictions extend to Users connecting to Cooper Union IT Systems with devices not owned by Cooper Union.

### SPECIFIC PROSCRIPTIONS ON USE

The following categories of use are inappropriate and prohibited:

- Users may not attempt to disguise their identity, the identity of their account, or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may not appropriate Cooper Union's name, network names, network number spaces, or Cooper Union logos, trademarks, or service marks. Users may not use the Cooper Union-assigned Internet number space for their own domain without IT's prior express permission.
- Users may not attempt to intercept, monitor, forge, alter or destroy other Users' communications. Users may not infringe upon the privacy of others' computers or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of the owner.
- Users may not engage in actions that disrupt or interfere with the legitimate use by other Users of any computers and/or networks, including the Cooper Union Network, that interfere with the supervisory or accounting functions of the IT Systems, or that are likely to have such effects. Such conduct includes but is not limited to placing of unlawful information on the system, transmitting data or programs likely to result in the loss of an individual's work or system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others, i.e., spam.
- Users may not possess, distribute, or send unlawful communications of any kind, including but not limited to threats of violence, obscenity, child pornography and/or harassing communications (as defined by law), or participate or facilitate communications in furtherance of other illegal activities.
- Users may not attempt to bypass computer or network security mechanisms, including the Cooper Union Network, without the prior express permission of the owner of that computer or network system. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt. The unauthorized scanning of the Cooper Union Network is also prohibited.

- Users must obey all established guidelines for any computers or networks used, both inside and outside Cooper Union. For example, individuals using computing resources provided by IT, The Cooper Union Library, individual Schools or Departments must adhere to the policies established for use of those resources. Users accessing off-campus computers via external networks must abide by the policies established by the off-campus owners of those computers and networks as well.
- Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permissions of the copyright holder. Information on the Digital Millennium Copyright Act can be found at: <http://www.copyright.gov/legislation/dmca.pdf> (PDF file) and the Copyright Act at: <http://www.copyright.gov/title17/>
- Users should refrain from using Cooper Union computing resources for personal commercial purposes or for personal financial or other gain. Personal use of Cooper Union computing resources for other purposes is permitted when it does not consume reasonable amounts of computing resources, does not interfere with the performance of the User's job or other College responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

## **AUTHORIZATION**

Users are entitled to access only elements of IT Systems consistent with their Specific Authorization. Upon request by a Systems Administrator or other College authority (e.g., Deans Offices, Human Resources, Business Office), Users will be granted access to the appropriate IT System. All User requests for access, as part of the onboarding and transfers will be communicated to IT via the Cooper Union ITM-Help Desk Application. Similarly, any terminations of access to IT Systems, including email, Colleague, etc. will be communicated to IT via the Cooper Union IT Help Desk Application. For new employees:

- Human Resources ("HR") determines and communicates a new User's (employee's) personnel classifications and job title to authorizing officials and IT, utilizing the appropriate procedures and workflows in the IT Helpdesk application.
- HR notifies IT via the Helpdesk application, which Systems Authority accesses and approves a User's (employee's) security classifications, access privileges, and hardware and software requisitions.

Upon hire, new administrative and academic Users receive standard hardware and software configurations. New employees may request amendments or additions, subject to approval by their supervisor and/or the System Administrator.

## **PERSONAL ACCOUNT RESPONSIBILITY**

Users are responsible for maintaining the security of their own IT Systems accounts and passwords and may not share passwords. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

## **ACCESS TO IT SYSTEMS AND USER-INSTALLED SOFTWARE**

No user-installed software may interfere with IT's ability to access any IT system.

## **AUTHORIZATION AND ASSIGNMENT OF INFORMATION SECURITY CLASSIFICATIONS**

Each Systems Authority/data area owner (HR, Finance, Financial Aid, Accounts Receivable, Admissions, Student Affairs, Budget, and Payroll) must approve access to student data and any financial applications, including Ellucian Colleague R18. The employee's supervisor, in conjunction with the appropriate authorizing official(s), must assign and approve information security classifications in accordance with the employee's job description. HR authorizes the appropriate forms and notifies IT to implement them via the IT Help Desk application. All access is reviewed yearly.

## **AUTHORIZATION/REQUESTS FOR MODIFIED INFORMATION SECURITY CLASSIFICATIONS**

When transfers and/or promotions occur, the Systems Authority must re-evaluate and modify the User's (employee's) information security classifications to match the User's (employee's) new position. Modification may include additional or partial removal of access. The Systems Authority will approve changes to access within the Ellucian Colleague System, including security class modifications, and HR will notify IT to implement them via the IT Help Desk application.

## **NOTIFICATION TO REVOKE USER ACCESS PRIVILEGES FOR TERMINATED EMPLOYEES**

When an employee is terminated, HR is responsible for communicating details of the IT Systems that require the removal of User privileges via the IT Helpdesk application. Unless HR specifies a particular date and time to revoke user privileges, IT will immediately disable the User's (employee's) access to all IT Systems, including the Ellucian Colleague R18 system (and, where appropriate, to any associated systems and platforms) upon receiving written notification of an employee's termination.

The employee must immediately return all Cooper Union-owned devices, equipment, media, credentials, and other IT resources in their possession or control. Cooper Union reserves the right to access, retain, review, and manage data stored on its systems in accordance with applicable law and institutional policy. Former employees remain subject to applicable confidentiality, data protection, and intellectual property obligations that survive termination of employment.

## **MONITORING**

Cooper Union may monitor, access, or review IT Systems, network traffic, and institutional data for legitimate operational, security, compliance, or legal purposes, consistent with applicable law. Such monitoring is intended to protect institutional systems, information, and operations and is not conducted for the purpose of surveillance of individual users or their activities. Monitoring activities will be conducted in a manner proportionate to risk, and access to user content will be limited to authorized personnel with a legitimate need to know.

## INCIDENT REPORTING REQUIREMENT

Users must promptly report suspected or confirmed security incidents, including phishing attempts, malware infections, suspicious account activity, lost or stolen devices, unauthorized disclosure of sensitive information, or other suspected compromise of Cooper Union IT Systems. Reports must be submitted immediately to the IT Help Desk or designated Information Security personnel.

## ENFORCEMENT

Penalties for violating the Cooper Union Acceptable Use Policy include restricted access or loss of access to the Cooper Union Network, termination and or expulsion from Cooper Union, and in some cases, civil and/or criminal liability.

Cooper Union reserves the right to update or revise the Acceptable Use Policy or implement additional policies in the future. Users are responsible for staying informed about Cooper Union policies regarding the use of computer and network resources and complying with all applicable policies.

## RELATED POLICIES, LAW AND REFERENCES

- Intellectual Property Policy
- Copyright Policy
- Employee Handbook and Code of Conduct
- Email Use Policy
- Data Privacy and related policies