PACE UNIVERSITY

Information Technology Services

Appropriate Use Policy for Information Technology

Table of Contents

01. Introduction

Identity of Information Technology Resources at Pace University ("IT Resources")

Information Technology (IT) at Pace University includes all campus computing, telecommunications, document services, educational media, and management information systems technologies. These IT Resources support the University's teaching, research, and administrative activities. Examples of IT Resources include, but are not limited to, the central administrative, academic, and library computing facilities, systems, and services—whether on-site or cloud-based; AI-powered tools, the campus-wide data, video, and voice network; electronic mail; conferencing systems; Internet access; voice mail; the University switchboard; fax machines; photocopiers; classroom audio-visual equipment; departmental and general-use computing facilities; computer and other related devices assigned to faculty, staff, and students; and related services. Pace's central information technology organization is "Information Technology Services" (ITS), led by the University's Chief Information Officer (CIO) and Vice President of Information Technology.

Appropriate Use of IT Resources

Users of IT Resources have access to valuable University resources, sensitive data, and external networks. Consequently, all users must act responsibly, ethically, and legally. Generally, "Appropriate Use" means understanding how to properly use Pace IT Resources, ensuring your use complies with it, respecting the rights of other Pace information technology users, preserving the integrity of the Resource, and following all relevant license and contractual agreements.

Scope

This Policy applies to any and all users of Pace University IT Resources, whether access occurs on-campus or remotely, and whether access occurs using University-owned devices or personally owned devices that connect to or access Pace IT Resources. Furthermore, this policy applies to all information technology owned or managed by Pace University and represents the minimum appropriate use standards for IT.

Key definitions (for purposes of this Policy)

- "University Data" means information created, received, maintained, stored, transmitted, or processed in connection with University business, including University records.
- "Restricted" and "Confidential" data mean University Data classified by the University as requiring heightened safeguards (including, as applicable, student education records subject to FERPA, health information, financial account information, authentication credentials, and other sensitive personal information). Please see the University *Data Classification Policy* in the University Policy Library for more details.
- "Public" data means information approved for public release.
- "Cloud Service" means any externally hosted service used to store, process, or transmit data (including SaaS).

02. Expectations for Appropriate Pace IT Use

The following list, while not exhaustive, sets forth expectations for appropriate and compliant use of Pace University's IT Resources:

A. Use Pace's IT Resources primarily for Pace University-related work. Limited, incidental personal use is permitted provided it (a) does not interfere with University operations, work responsibilities, academic activities, or other users; (b) does not incur more than minimal additional cost to the University; (c) complies with applicable law and University policy; and (d) is not for personal financial gain, outside commercial activity, or other–than-Pace business work.

B. Pace University encourages information technology literacy for its students, faculty, and staff. Use of University-provided email and other collaboration services for limited, incidental personal use is permitted as described in item A above. Personal use must not violate this Policy, must not involve personal or financial gain, and must not imply University endorsement.

C. Only use the IT Resources for which you have been granted specific authorization. It is strictly prohibited to use another person's ID or account or to attempt to access other users' passwords. Users are individually responsible for all activities involving their assigned resources; therefore, sharing IDs is not allowed.

D. Follow established guidelines for all IT Resources used both on campus and off. For example, individuals using Pace's computer labs, computer classrooms, and public-access computers must adhere to the policies set for those devices; those accessing off-campus computers through external networks must comply with the policies established by the system owners and the rules governing the use of those networks.

E. Do not attempt to modify, delete, or destroy any software on any Pace IT Resource. This violates the proper use of IT Resources, regardless of how weak the protection is on those products.

F. Users are responsible for all activity conducted under their accounts and must comply with all applicable state and federal laws and University policies when using IT Resources.

G. Digital content you create, post, distribute, or use in connection with University programs and services (including websites, documents, instructional materials, and multimedia) must comply with commonly accepted accessibility standards, such as the most recent version of the Web Content Accessibility Guidelines (WCAG).

H. Respect others' privacy and personal rights. Do not access or copy another user's email, data, programs, or files without permission. Pace endorses the following statement on software and intellectual property rights distributed by EDUCAUSE, the non-profit consortium of colleges and universities dedicated to managing information technology in higher education. The statement reads:

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to the work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access and trade secret

and copyright violations, may be grounds for sanctions against members of the academic community.

I. The University policies on plagiarism or collusion apply to the use of IT Resources in course assignments.

J. The Higher Education Act requires institutions to create plans that provide students with legal options for downloading music and movies, as well as exploring technologies to prevent illegal peer-to-peer file sharing. Pace University's official stance on peer-to-peer (P2P) file-sharing software is that the software itself is neither illegal nor prohibited by Pace University. However, it is illegal to download or share copyrighted material for which you do not hold the rights. All Pace users must respect copyrighted content accessible through the Pace network. Any violation of copyright can result in disciplinary actions and legal consequences.

Rulings by courts under the Digital Millennium Copyright Act have determined that Internet Service Providers, or ISPs (for example, Pace University, which acts as an ISP for its students, faculty, and staff), must disclose the identity of users associated with specific Internet Protocol addresses or "user IDs" listed above when presented with a properly issued subpoena. Individual students, faculty, and staff can be held personally liable for copyright law violations.

Visit the Illegal File Sharing website for more information.

K. You must comply with all relevant copyright laws and licenses. Both University policies and the law explicitly prohibit copying software that is not in the public domain and distributed as "Freeware" or "Shareware." Users are expected to follow the terms of shareware agreements. ITS will maintain University-wide site licenses.

L. To avoid risking the University's tax-exempt status, do not use Pace IT Resources for personal financial purposes or political activities without prior written approval in each case. Contact the CIO/Vice President of Information Technology (cio@pace.edu) for detailed information.

M. Use appropriate standards of civility and common sense when using IT Resources to communicate with other individuals. Do not post to public websites or use e-mail to transmit confidential information relative to personnel matters, internal investigations, and ongoing or threatened litigation, or information containing Personally Identifiable Information such as Social Security Numbers, Bank Account Numbers, Credit Card Information, and Health Information. When sending personal messages to other users, participating in a Chat Room discussion, posting on electronic bulletin boards, or leaving a voice mail message, identify yourself as the sender. Using Pace's IT Resources to harass, slur, embarrass, or demean other individuals is explicitly prohibited.

N. Be considerate of others' needs and only use your fair share (what a reasonable person would consider fair) of IT Resources. For example, users of shared resources, such as public access computers, should use these facilities only for the most essential tasks during peak periods. Broadcasting non-critical messages to large groups (spamming) and sending chain letters are activities that cause network congestion, disrupt others' work, and are prohibited.

O. Treat IT Resources and electronic information as a valuable University resource. Protect your data and the systems you use. For example, ensure that you back up your files regularly using university-approved backup solutions.

P. Users must protect their University credentials and accounts. They should not share passwords or approve multi-factor authentication (MFA) prompts for others. MFA is mandatory where the University requires it and is necessary to access key University systems and Restricted or Confidential University Data. Users must not approve unexpected or suspicious MFA prompts and must report such activity immediately to Information Technology Services (ITS). Passwords must meet Pace's Password Policy, including minimum length, complexity, and other requirements—such as screening against common or compromised passwords. Users must follow University authentication and account management procedures, including password changes, credential recovery, and account lockout. More information about good password practices is available at the Password Security webpage and in the University's *Password Policy* in the University Policy Library.

Q. Make sure you understand the access privileges you've assigned to your files. Do not damage or destroy any IT Resources. Devices used to access Pace IT Resources must run supported operating systems, apply security updates promptly, and use basic security measures such as a screen lock. When required by University standards (including for access to Restricted or Confidential data), devices must use encryption and University-approved endpoint protection. Jailbroken or rooted devices must not be used to access University systems that handle Restricted or Confidential data. Deliberately introducing malicious computer code, such as viruses and worms, into the Pace University computing environment or spreading them through Pace's network to other systems violates University standards and regulations.

R. Stay informed about the Pace IT environment, as it is constantly evolving to keep up with academia and the needs of our students. Pace shares information through various channels, including the ITS website, IT Status Page, the Pace Home Page, the ITS Newsletter, logon messages, email alerts/notices, online documentation about policies and procedures, published University newsletters, and meetings. Users are responsible for staying updated on these changes and are expected to adapt to shifts in the University IT environment.

S. All users share the responsibility for protecting the confidentiality, integrity, and availability of Pace University's information technology resources and data. Users are expected to stay vigilant and informed about common information security threats—including phishing and other social engineering scams, malware, account compromises, and unauthorized data disclosures—and to exercise good judgment when using email, messaging platforms, cloud services, and online resources. Users must be careful when opening links or attachments, verifying requests for sensitive information, and responding to unexpected or urgent messages, even if they seem to come from trusted sources. Information security is a team effort: users should promptly report any suspected phishing messages, security incidents, or unusual system activity, follow University security policies and training, and take reasonable steps to protect their accounts, devices, and data. By working together, members of the University community help protect Pace's academic mission, operations, and shared digital environment.

T. The following guidelines have been established regarding University-related use of online publishing, collaboration, and social platforms (including but not limited to blogs, wikis, discussion forums, social media, and other externally hosted collaboration tools) by faculty and staff:

   i. Faculty and staff members may request a blog for use in conjunction with their work. The requestor will be the owner of the blog and assumes responsibilities as defined in this Appropriate Use Policy.
   ii. Faculty and staff members may also request group blogs. Group blogs can be used in courses, research, department websites, and collaborative projects.

iii. Faculty and staff members may request additional Pace computer accounts for collaborators from other institutions, and their use will be covered by this Appropriate Use Policy.
iv. Anonymous postings to blogs and wikis are not permitted. Owners of blogs may not reconfigure the system to allow anonymous postings.
v. All comments will be run through a SPAM engine. An individual making a comment is required to provide a valid email address before entering comments. The blog owner is responsible for reviewing each comment before posting it to the blog for others to see. The blog owner reserves the right not to publish individual comments. The blog owner may opt to require Pace password authentication before comments can be submitted.
vi. Blogs created by Pace-provided software/system will be listed on a web page and be available for RSS syndication.
vii. Pace does not guarantee that it will provide ancillary software, such as databases and script languages, that authors may wish to use in their blogs.

U. All suspected information security incidents must be reported as quickly as possible, and within six hours of learning about the incident, through appropriate channels, including the Information Security Office (iso@pace.edu). If you are unsure whether an event is an incident, report it. Notification should be made to the Information Security Office (iso@pace.edu), and where appropriate, to the local campus office of University Safety and Security, University Counsel, and/or the Risk Management Department. All parties have a duty to report information security violations and issues promptly so that quick remedial actions can be taken. Please see the *Incident Reporting Policy* in the University Policy Library for more information.

V. Staff and faculty who record online webinars, lectures, and similar sessions that will be posted on publicly accessible websites (i.e., without login required) must notify participants before attending and again at the start of the event that the session will be recorded and later made available publicly. Contact Educational Media for the correct language and procedures to follow. Participants in online webinars, lectures, etc., are not allowed to make recordings unless prior permission is granted by the presenter(s) and/or sponsor(s).

W. University business must be conducted using a University-issued non-student email account. The use of personally owned, third-party, or other non-Pace-issued accounts for University business is prohibited. Only University-operated and approved cloud-based applications linked to University-issued accounts may be used to store, process, or share University Data. Users must apply appropriate sharing controls, including least-privilege access and limiting public or anonymous sharing, when sharing University Data. Restricted or Confidential University Data must not be stored or shared using unapproved services (e.g., Google, DropBox, Box, etc.) or personal accounts. Please contact ITS for more information on approved applications for safe and secure cloud-based document storage and sharing.

03. Use of AI Tools

When using tools that include Artificial Intelligence (AI) technology (“AI Tools”), including, but not limited to, generative AI tools (such as ChatGPT, Microsoft Copilot, Google Gemini, Claude, etc.) for University business, users must comply with this Policy and applicable University guidance.

- Where required by University, course, program, or departmental rules, users must disclose material use of AI Tools and comply with applicable academic integrity requirements, including

the University's AI Academic Policy, Academic Integrity Code and/or Honor Code for Law School Students. Please see the University's AI Resources page for more information.

- Users must not input, upload, or otherwise provide Restricted, Confidential, or any other sensitive University Data into public or unapproved AI Tools. Restricted or Confidential University Data includes, without limitation: student education records subject to FERPA; health information; Social Security Numbers; payment card data; bank account information; authentication credentials (including passwords, tokens, MFA codes/prompts); export-controlled or sponsor-restricted research data; donor/alumni data; applicant/admissions data; and employee personnel/HR data. Please see the University *Data Classification Policy* in the University Policy Library for more details.
- Where the University provides or approves an AI Tool for University use, users must use the University-approved tool for University business involving University Data and must follow any applicable configuration requirements.
- Users must not use an AI Tool for University business if the tool's terms or configuration permit the provider to train on, claim rights to, or retain user inputs/outputs in a manner inconsistent with University requirements, unless the tool has been reviewed and approved by the University through ITS and appropriate contractual processes.
- AI outputs must not be used without human review to make or support decisions with significant impact on individuals (e.g., grading/academic standing, student advising decisions, disciplinary matters, employment actions, financial decisions, or official University communications).
- Users remain responsible for reviewing and verifying AI outputs for accuracy, appropriateness, bias, and compliance before use; AI outputs used for University purposes must be handled, stored, and shared as University Data and only in approved systems.
- Users must not use AI Tools to circumvent security controls, violate law or policy, generate or distribute malicious code, conduct unauthorized scanning/testing, or automate bulk actions (e.g., mass emailing/messaging, scraping, or account creation) that interfere with University systems or other users.
- Users may not install, configure, or run agentic AI systems on University-owned devices or within the Pace network that are capable of accessing local files, folders, system credentials, password stores, email, or other protected institutional data without explicit authorization from ITS. Such tools may autonomously read, modify, transmit, or store University information and therefore present significant security and privacy risks. Installation or use of these systems on Pace-managed computers or accounts is strictly prohibited unless formally approved through ITS security and governance review.

04. Access to IT Resources

Central IT Resources

Students, faculty, administrators, staff, recognized student organizations, and approved external users may obtain IDs for use in central IT activities related to instruction, research, or University administration. Students employed by the University will receive a separate user account to be used for University business.

If any member of the University or an approved external user leaves, resigns, or ends their relationship with Pace University for any reason, access to all IT Resources, including but not limited to voicemail, email services, and files stored on university computers (such as desktops and file shares), will be terminated promptly in accordance with University processes and system controls. Accounts are automatically created and deactivated based on information in the University's system of record

(currently, Banner) and are in accordance with applicable university and departmental policies and procedures.

Qualified retirees (as defined by Human Resources) may request a retiree email account, which will be separate and distinct from the account previously assigned as a faculty or staff member.

To enable students to communicate with faculty, complete assignments, and receive required notifications, student e-mail accounts will be deactivated 12 months after the last class taken.

Other IT Resources

Most of Pace's IT facilities and services—such as the computer labs, classrooms equipped with computers, Video Conferencing rooms, consulting services, voicemail, and training—are available to members of the University community. ITS plans and budgets for central IT services. However, these services are not free. Users or departments may be required to cover the additional costs for excess usage (based on typical, normal utilization) or for abuses of Pace IT resources (expenses beyond the baseline budget). For more detailed information about access to any facility or service, visit the ITS homepage.

Departmental IT Resources

For information concerning access to departmental IT resources, contact your department's IT staff or Department Chair.

05. Data Security and Integrity

ITS-Maintained Equipment

ITS offers reasonable security against intrusion and damage to files stored in the central IT facilities. ITS also provides some tools for archiving and retrieving files specified by users and for recovering files after accidental data loss. However, other users cannot hold the University or any IT staff accountable for unauthorized access, nor can they guarantee protection against media failure, fire, floods, etc. Users should employ all available methods to protect their files, including frequently changing passwords and using University-approved backup tools to back up data. If data becomes corrupted due to intrusion, ITS should be notified immediately. Every reasonable effort will be made to restore files to their pre-intrusion state; however, ITS cannot guarantee recovery.

Upon request, the IT staff will assist in implementing procedures to enhance security. Although ITS backs up some departmental servers and makes reasonable efforts to protect them from intrusion, it does not provide the same level of protection or offer file restoration for files stored on departmental servers. Therefore, it is especially important for users to back up their files and utilize all available methods to safeguard their data on departmental systems.

The central Pace information technology organization (Information Technology Services, ITS), led by the University's Chief Information Officer/VP, Information Technology, reserves the right to manage the University's voice, data, and video bandwidth. Criteria for bandwidth management involve the integrity and robustness of University-owned equipment, data, and services as well as the appropriateness of bandwidth use in relation to the University's academic goals, administrative missions, and this Acceptable Use Policy for Information Technology.

Departmental Facilities

Data security and integrity in departmental IT facilities vary depending on the department. Users should contact their department's IT staff for more information on their security and data integrity procedures.

06. Privacy

To ensure compliance with Pace University's internal policies, applicable laws and regulations, and to maintain the security and integrity of University systems, as well as to ensure the safety of employees and the community, Pace University reserves the right to monitor, inspect, access, or search its information systems (including the contents of University-provided email accounts, systems, and storage) at any time, in accordance with applicable law and University procedures. Access to user content for investigative or administrative purposes will be limited to authorized personnel with a legitimate University purpose and may require approval, documentation, and logging as required by the University.

Pace University management reserves the right to remove any material from its information systems that it considers offensive, potentially illegal, or otherwise against University policies.

Access by IT Staff on Behalf of the University

Although not legally required, the University respects the privacy of all users. However, it should be understood that all data created or stored on University systems and IT Resources is the property of Pace University. Members of the ITS organization are forbidden to log into another user's account or access a user's files, software, or other contents unless the user grants explicit permission (for example, by setting file access privileges). Exceptions to this privacy policy are made under specific conditions. These include investigating programs suspected of causing network disruptions or other shared services, other internal investigations, examining suspected violations of state or federal law or University policies, and conducting investigations to prevent liability or in connection with internal hearings or litigation.

Before accessing a user's account, files, software, or other content, reasonable efforts will be made to notify the user, except when such prior notice would violate legal requirements, directives, or jeopardize an internal investigation. In those cases, before examining a user's account, files, software, or other content, the Vice President of Information Technology or their designee, after consulting with University Counsel, must determine that there is a legal obligation or other sufficient cause to do so without prior notice or permission from the user. Information obtained this way is admissible in legal proceedings or in a University internal investigation or hearing. All parties involved will keep information regarding security incidents and investigations confidential. Only authorized personnel may disclose such information. By accepting a user account, the user agrees to this policy.

Access by Administrators of Departmental IT Systems

Departmental IT staff should not access a user's files without that user's explicit permission or monitor file traffic in a way that allows intrusion into the file contents. However, some exceptions may be necessary, such as when a file is suspected of disrupting the local network or other shared services and the user cannot be reached. Additionally, information about system users and data stored by them should be kept confidential. Individual departments may have guidelines aligned with University policy that address access to their IT resources.

Electronic Communications

Users should not expect privacy for any electronic communications. IT systems administrators may view the contents of electronic messages due to serious addressing mistakes or when maintaining the communications system. In cases where administrators do see the contents of private electronic messages, they are required to keep the contents confidential. Users should also understand that the current design of the networks means that the privacy of electronic communications leaving Pace cannot be guaranteed. Additionally, when a user's association with Pace ends, any emails received at Pace addressed to the former user will either be returned to the sender or, if appropriate, forwarded for a limited time to an address specified by the former user or their supervisor.

07. Ownership of Copyright for Materials Developed with Pace's Resources

Pace University has established guidelines related to ownership of copyright property. The exact policies and procedures relating to copyrights are in the Pace Faculty Handbook at pp. 61-71 and the Pace Copyright Policy and Procedures. Finance and Administration | Copyright Policy and Procedures | Pace University New York

08. Responsibility for Errors in Software, Hardware, and Consulting

ITS strives to maintain an error-free IT environment for users and to ensure that the IT staff is properly trained. However, it is impossible to guarantee that IT system errors will not occur or that IT staff will always provide correct advice. Pace offers no warranty, either expressly stated or implied, for the services provided. Damages resulting directly or indirectly from the use of these resources are the user's responsibility. However, upon the user's request, when errors are identified on IT facilities, members of the IT staff will make a reasonable effort to restore lost University information to its state prior to the failure. As part of maintaining the IT environment, the IT staff applies vendor-supplied or locally developed fixes as appropriate when problems are identified. Since vendors may be involved and staff resources are limited, no guarantee can be made about how long it may take to resolve an error once identified.

When software errors are considered major problems or could produce inaccurate results, users will be notified as soon as possible using appropriate electronic and/or other media.

09. Changes in the Pace IT Environment

When significant changes in hardware, software, or procedures are planned, notifications will be sent via email and other channels to ensure all users have enough time to prepare and voice any concerns they may have.

10. Non-Compliance

All users of Pace University's IT Resources must adhere to this Appropriate Use Policy for Information Technology, all other IT policies, and the University's Guiding Principles of Conduct related to the use of the University's IT resources. Failure to comply with any of these policies may lead to temporary or permanent revocation of system or network access, notification to the user's supervisor, and/or disciplinary actions, up to and including termination of employment or dismissal from the University, in accordance with applicable University policies and procedures (such as Student Conduct policies, faculty handbook processes, and Human Resources policies). When relevant, a violation may also result in civil and/or criminal liability and could be referred to law enforcement.

11. Comments, Suggestions, Corrections, etc.

Questions concerning this or any other Information Technology Policy can be directed to the ITS Customer Support Center via helpdesk.

12. Revision History

Version	Date	Change	Author
1.0	4/24/2018	Previous version converted into official policy template. Policy reviewed and updates made to password and email sections.	CE
1.1	5/11/2018	Formatted	DM
1.2	10/28/19	Fixed Broken Links	CE
1.3	11/29/19	Additional edits in various sections	CE
1.4	2/22/21	Added clarifications on email and third-party document sharing sites. University Counsel review and approval	CE/ PD/ SB
1.5	4/21/2022	Added clarifications in section 5 and updates to student email account termination.	CE/ PD/ LV
1.6	4/15/2024	Review and updates – added section on AI	CE/ BG/ CB/ AK
1/7	4/15/2026	Review, substantial grammatical updates, expanded section on AI	CE/ BG/ CB/ DB/ MW

13. Disclaimer Statement

Pace University reserves the right to amend or otherwise revise this document as may be necessary to reflect future changes made to the IT environment. You are responsible for reviewing this Policy periodically to ensure your continued compliance with all Pace University IT guidelines.