Acceptable Use Policy

Accommodations for individuals with disabilities in accessing these policies are available upon request by emailing accessiblepolicy@wcupa.edu

Purpose and Scope

The Acceptable Use Policy for West Chester University Information Services & Technology computing facilities, systems and resources applies to all members of the University community, including faculty, students, staff, contractors, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access service or eduroam access, and to those who register their computers and other devices through Conference Services programs or through other offices, for use of the campus network.

Policy Statement

Access to the University's computing and information system network and resources is a privilege granted solely to the University's faculty, staff, students, and those other individuals who have been approved for special accounts. The intent of the University in granting access to individuals is to support the academic mission of the University, to share information and ideas and to manage its administrative and service operations and activities. Obtaining and maintaining an electronic account is a privilege, not a right. All users must show responsibility and proper judgment when using their University account or network in order to protect the integrity of University data, network, and resources.

While the University respects the individual's right to free speech and free expression, using university facilities, systems and technology resources are intended to be utilized for academic pursuits or university business and it is expected that the use of these systems will fall within the guidelines of generally accepted professional standards of the University and responsible use of technology resources by all members of the campus community. This Policy applies to collaborative platforms (such as, but not limited to, Zoom & Microsoft Teams). The University reserves the right to limit or revoke electronic account privileges for misuse or abuse of those privileges. Agreement to abide by this policy is a condition of acceptance to use the University's computing and information network facilities and resources.

While the university recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned information technology, except as required by state or federal law. For example, the university may be required to provide information stored in its information technology resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute. Information stored by the University may also be viewed by technical staff working to resolve technical issues.

While the University does not routinely examine these files or monitor their content, there is no expectation of privacy in using WCU IT resources. WCU reserves the right to inspect, monitor, and disclose all IT resources including files, data, programs, and electronic communications records without notice to or the consent of the holder of such records.

Procedures

Protecting Data - University data and information systems are its most valuable assets. Information must be safeguarded for reasons of data integrity, confidentiality, and availability. The following rules must be observed:

- IS&T (Information Services & Technology) will not issue or endorse the use of shared, departmental accounts, except in rare cases where justification has been established and the Information Security Office approves proposed management processes.
- Never share a password or Multi Factor Authentication (MFA) codes with another person.
- Never attempt to discover or use another individual's password or network ID.
- Never attempt to circumvent data protection schemes or uncover security loopholes.
- Never attempt to monitor another user's data communications, or attempt to read, copy, change, delete or transmit another user's files without their expressed written permission.
- Never attempt to gain unauthorized access to remote computers. Remote work/access should always be conducted using University approved methods and applications (Connecting via the Virtual Private Network (VPN) and with secure applications such as Windows Remote Desktop, SSH, etc. with IS&T review and approval).
- Always protect removable media (USB drives, DVDs, etc.) by securing them immediately after use.
- Always use University governed cloud storage (Microsoft 365, primarily OneDrive for Business) to save university data. All University data should be stored securely, as appropriate for the security classification of the data.
- Always log out of sessions when not in use

- Monitor access to accounts and attempted log-ins. If a user suspects that their University account has been compromised or that there has been unauthorized activity on their accounts, they are to report it to the IS&T Help Desk immediately and change account password.

E-Mail - University e-mail account-holders can generally expect that the content of e-mail files residing in their user accounts will be treated as confidential by the University. The University does not routinely examine these files or monitor their content. Under certain circumstances, however, e-mail can lose its confidentiality. It can be lost if the University is compelled by court order to be released, by signed release from the user, if the files are transmitted by the user to others and user custody is lost, or when such information is deemed by University officials to be of evidentiary interest to a disciplinary investigation. Under these specific circumstances, e-mail privacy cannot be guaranteed by the University. Users should be cognizant of the lack of expectation of privacy under these circumstances. The following rules must be observed:

- Never send or forward unsolicited or phishing email, except to report malicious messages to IS&T Help Desk.
- Do not open attachments you were not expecting to receive. Unsolicited email attachments are a popular way of distributing viruses and malware.
- The use of your account or University computing and information system network for personal business purposes is prohibited.
- Never send harassing, threatening, defamatory, or fraudulent messages or images to others.
- Never provide personal information to suspicious e-mail.
- Unsolicited job offers or winning contests you never entered that appear too good to be true, usually are.
- Delete e-mails that do not require preservation.

Ownership and Use of IS&T Facilities and Resources – Information Technology resources may be acquired by the University through lease, purchase, license, loan, or other agreement. Information Technology resources may include, but are not limited to, computers, accounts, workstations, mobile devices, printers, software, servers, and systems, as well as related devices and hardware and telecommunications equipment. Ownership lies exclusively with the University, not the user. The University has established the following rules associated with the use of its computing and information technology facilities and resources. They must be observed:

- The installation of unapproved software is strictly prohibited.
- Never run or install a program that could intentionally result in damage to or destruction of data, a computer system or information network. The willful introduction of viruses, malware, monitoring programs, and other malicious software are expressly prohibited.
- Never be wasteful of computing or information network assets or unfairly monopolize these resources. Waste in the form of unauthorized mass mailings, cryptocurrency mining, unnecessary printing output, or creating unnecessary network traffic are expressly prohibited.
- Never engage in behavior that could impair or impact the operation of computers, peripherals, or networks. Acts such as tampering with the local area network (LAN), wireless networks, the high-speed network backbone, or otherwise blocking communication lines or interfering with the operational readiness of a computer are expressly prohibited.
- Never use the University's devices or information networks for financial gain or other personal benefit, or for other reasons that result in a direct cost to the University.

- Never abuse work hours by spending large amounts of time in pursuit of social or other non-business-related personal interests that utilize the University's information technology facilities and resources. (Examples of this include social media, sexually explicit sites, sports fantasy, and video-sharing sites.)
- Never store or attempt to download or otherwise transmit data that would constitute a violation of state or federal law or the policies of the University, the State System of Higher Education, or the Commonwealth of Pennsylvania.
- The installation and use of pirated or unlicensed software on University-owned systems is prohibited. Users are not permitted to install any software on University computers or mobile devices without authorized software licenses and must abide by the terms of the respective software license agreements. Unauthorized duplication of software is illegal and expressly prohibited.

Non-University owned devices (BYOD): Faculty, staff, students, and guests of West Chester University who provide their own computer and equipment to connect to the University's network must still abide by all aspects of the Acceptable Use Policy. In addition:

- Responsibility: The user's personal device and the content of any files or services made available to others over the network is the sole responsibility of the person with ownership of and/or administrative authority over the device providing the service. This person is responsible for being aware of all applicable federal and state laws and University policies. This person will be liable for any violations of these laws and policies.
- Network-intensive applications: Any person operating a network-intensive application, or a device compromised by malware, which causes network overload or unauthorized access attempts to other systems/servers, will be notified and steps will be taken to protect other users and the University network overall. This may include disconnecting the offending device from the

network until the problem is resolved. If the condition is an imminent hazard to the University network or disrupts the activities of others, then the offending device or the subnet to which it is attached may be disabled without notice. This latter course of action may affect other users connected to the network.

- Responsibility for security: Any person attaching a device to West Chester University's network is responsible for the security of the device and for any intentional or unintentional activities from or to those network connections.
- Wireless Equipment: The use of any type of wireless network equipment including but not limited to wireless switches and wireless routers on the University network is strictly prohibited. Only wireless access points installed and managed by the West Chester University Information Services & Technology will be allowed in use on the University's network. Information Services will maintain a current list of wireless access points available on the network.
- Ethernet Network: Network services and wiring may not be modified or extended by users for any reason. This applies to all network wiring, hardware, and data jacks. Ethernet switching equipment and hubs other than those provided by the University are prohibited for use on any West Chester University network without prior written approval from the Executive Director of IT Infrastructure Services.

Violations and Misconduct

Minor Infractions – The Information Security Office will contact the user/system owner, advising them of the violation, implementing a solution to obtain assurance from the user that the action will not be repeated.

Serious Misconduct by Employee – Everyone has a responsibility to report these types of acts if witnessed or suspected. Serious and intentional misconduct will be immediately addressed by the Information Security Office to investigate misuse of computing and information technology facilities and resources.

- Reporting Suspected Misuse or Other Violation of this Policy: Instances of alleged misuse/violation should be reported to the University's IS&T Help Desk immediately. The IS&T Help Desk will make an effort to resolve the situation or, if necessary, refer the concern to the Senior Associate VP & CIO of Information Services & Technology and/or Chief Information Security Officer for further review and action.
- Additional Notifications: Anytime employee misconduct is alleged, the Chief Human Resources Officer and the Department of Public Safety must be notified immediately by the Senior Associate VP & CIO of Information Services & Technology and/or Chief Information Security Officer. If the allegation might reasonably lead to a criminal complaint, the department of Public Safety will take over the investigation. If the allegation relates to possible sexual harassment or another form of illegal discrimination, the Chief Human Resources Officer will notify the Chief Diversity and Inclusion Officer immediately. Notice to the employee who is the subject of the investigation shall be made by the appropriate University official after consultation with the Chief Human Resources Officer.
- Decision to Investigate: The Senior Associate VP & CIO of Information Services & Technology and/or The Chief Information Security Officer, in consultation with the Chief Human Resources Officer and other appropriate University officials, will review the concern and determine how to best approach the conduct of a thorough investigation prior to investigatory action being undertaken by the campus.
- Privacy Interests: Every reasonable effort will be made by the Senior Associate VP & CIO of Information Services & Technology and/or Chief Information Security Officer and any others involved in an investigation pursuant to this policy to balance a minimization of intrusion upon employee privacy interests while responsibly conducting a complete investigation. West Chester University

and PASSHE (Pennsylvania State System of Higher Education) legal counsel will be consulted if questions arise in this regard.

- Collective Bargaining Agreements: The Chief Human Resources Officer will be consulted regarding employee collective bargaining rights relating to investigations and pre-disciplinary meetings if the subject of a complaint is a member of a collective bargaining unit.
- Suspension of User Privileges: There may be circumstances where the nature of an allegation is so serious as to require a suspension of privileges while an investigation is being conducted. Under these circumstances, both the employee and the union (where applicable), will be notified at the time of the suspension. Suspension of user privileges pending the outcome of an investigation is not a disciplinary action.

Serious Misconduct by Student –Unfortunately, from time to time, computer or network abuse, electronic harassment, and other unauthorized acts do occur. When this happens, these must be effectively managed to avoid recurrences. Everyone has a responsibility to report these types of acts if witnessed or suspected. Given such notice, the University and Information Security Office has an obligation to investigate misuse of computing and information technology facilities and resources.

- Reporting Suspected Misuse or Other Violation of this Policy: Instances of alleged misuse/violation should be reported to the University's IS&T Help Desk immediately. The IS&T Help Desk will determine either to make an effort to resolve the situation or, if necessary, refer the concern to the Chief Information Security Officer and/or Senior Associate VP & CIO of Information Services & Technology for further review and action.
- Additional Notifications: Anytime student misconduct is alleged, the Chief Information Security Officer will notify the Office of Student Conduct via their reporting form - https://www.wcupa.edu/report. The Chief Information Security

Officer will also notify the Department of Public Safety. If the allegation might reasonably lead to a criminal complaint, the department of Public Safety will take over the investigation. If the allegation relates to possible sexual harassment or another form of illegal discrimination, the Chief Human Resources Officer and/or Sr. Associate Vice President will notify the Vice President of Student Affairs immediately. Notice to the student who is the subject of the investigation shall be made by the appropriate University official after consultation with the Division of Student Affairs. who is the subject of the investigation shall be made by the appropriate University official after consultation with the Division of Student Affairs.

- Decision to Investigate: The Senior Associate VP & CIO of Information Services and/or Chief Information Security Officer, in consultation with the Division of Student Affairs and other appropriate University officials, will review the concern and determine how to best approach the conduct of a thorough investigation prior to investigatory action being undertaken by the campus.
- Privacy Interests: Every reasonable effort will be made by the Chief Information Security Officer and any others involved in an investigation pursuant to this policy to balance a minimization of intrusion upon student privacy interests while responsibly conducting a complete investigation. West Chester University and PASSHE legal counsel will be consulted if questions arise in this regard.
- Suspension of User Privileges: There may be circumstances where the nature of an allegation is so serious as to require a suspension of privileges while an investigation is being conducted. Under these circumstances, the student will be notified at the time of the suspension. Suspension of user privileges pending the outcome of an investigation is not a disciplinary action.

Outside Investigations - Occasionally requests from local, state, or federal agencies will be made to investigate or provide information about technology related resources. These could include but not limited to server logs, email transactions, or user information. These requests will be routed through either the Department of Public Safety or the Information Security Office. Once a request is made to either department, the other respective department will be notified as well, unless it would compromise the integrity of the investigation.

<u>Litigation Requests</u> – As part of an independent Commonweath agency, West Chester University users' email, chat, and organizational data are considered public records, and therefore subject to Right-To-Know requests at any time. The communication records and data of users may also be subject to collection, retention, and sharing if the user is named in any form of litigation against the University. Users may, or may not, be informed of record/data collection.

<u>Disciplinary Consequences</u> - Verified, serious misuse or repeated, minor infractions of this policy will result in disciplinary action. The typical form of disciplinary action for non-criminal offenses is loss or restriction of privileges, although other forms of discipline which would be more appropriate under the circumstances are possible. Under normal circumstances, disciplinary actions will be issued by the department director or by the University official charged with that responsibility as part of the collective bargaining relationship.

<u>Statutory Violations</u> - Some instances of misuse may also rise to the level of violation of the Commonwealth's unfair trade practice, consumer protections and telecommunications laws, the Crimes Code of Pennsylvania and a variety of other state and federal laws. They include prohibitions against such conduct as disruption of services, computer theft, computer trespass, distribution of viruses, unlawful transmission of e-mail, exploitation of children via the Internet, or unsolicited or misleading transmission of commercial e-mail, faxes, or mobile telephone messaging

systems. Further information or copies of these statutes may be obtained from the Information Security Office.

Definitions

Acceptable Use - Use of University's computing facilities and resources must be consistent with the mission of the University and all applicable laws and policies. For use to be acceptable, it must demonstrate awareness and sensitivity towards the intent of the University in granting users' access, the coexisting privileges of other users, privacy interests and freedom from harassment or annoyance, the intellectual property rights of others, and the ownership and confidentiality of data

BYOD – Bring Your Own Device; terminology commonly used for utilizing personally owned devices on University network and/or for accessing and storage of institutional data.

Reviewed by: **Information Services & Technology**

Policy Owner: **Steve Safranek**
Chief Information Security Officer
Information Services & Technology

Office of Labor Relations Review: Review completed December 27, 2022

Approved by:
JT Singh
Senior Associate VP & CIO

Information Services & Technology

Date: October 13, 2023

Effective Date: October 13, 2023

Next Review Date: October 13, 2027

History:

11/29/2017 - IS&T Update, approved by VP, Information Services & Technology

2/12/2021 - Updated to WCU Policy Template

10/7/2022 - IS&T Update

10/13/2023 - IS&T update

11/30/2023 - Minor formatting update and publish.r

Initial Approval: 3/6/2007