INFORMATION SECURITY & RESOURCE USE POLICY

WWC ITS

Rev 2020-06-10

The purpose of this statement is to establish policies and procedures that promote the security and integrity of the college's computer and network systems, the information contained on those systems, and to provide a framework for responsible access to computing and information resources. Warren Wilson College extends these principles and guidelines to systems outside the college which are accessed via the college's facilities. Computing or network providers outside Warren Wilson College may impose their own additional conditions of appropriate use, for which users at Warren Wilson College are responsible.

Responsibilities of the User

Utilization of any college information technology facility including access to an account constitutes acceptance of the terms of this policy. Users acknowledge they have read and understand this policy and they shall be personally responsible for their acts or omissions in connection with utilization in violation of this policy.

ALL USERS

- All users must abide by current security guidance as it pertains to password strength, multi-factor authentication requirements, etc.
- Credentials must always be stored & transmitted securely (e.g. not in plain text, sent over chat/email, nor hardcopy records at workstations).
- NEVER transmit or share passwords to college resources or accounts for any reason. Neither ITS nor anyone at the college should ever ask a user for their password and users should not share their passwords.
- Log off or lock user sessions at all times when physically away from devices.
- All users are expected to carefully scrutinize all incoming communication such as email, calls, texts to avoid phishing and other access scams. See ITS training for information on how to spot common tactics.
- **Any potential breach regardless of scale must be reported to ITS immediately.**

USING COLLEGE-OWNED DEVICES

- Any College owned devices must remain with the assigned users and are not to be loaned or traded without explicit ITS approval & involvement.
- Endpoint protections including antivirus, security policy, permissions or other configurations may not be disabled or adjusted.
- Any changes to hardware or software must be approved & coordinated with ITS in advance.
- The user shall exercise care in the use of any college-owned equipment and to assure against theft of college owned equipment. Appropriately securing work areas or mobile devices to help assure against theft is both an individual and community responsibility. Damage or loss of equipment due to negligence or misuse may result in the cost being passed to the user. Any lost or stolen devices must be reported to ITS & Public Safety immediately.
- Avoid plugging in outside devices except where approved by ITS.

- Avoid personal interests on work devices.

SENSITIVE DATA USERS
(sensitive data is defined at end)

- Only College-owned devices may be used for work that includes sensitive data and/or accessing privileged systems.
- Where whole-disk encryption is not utilized, sensitive data must be stored only in approved locations such as IT-designated Cloud or server-based file shares and not on local drives. Locations used to store temporary data such as download, document or desktop folders should be regularly purged.
- Users of this type will be subject to additional restrictions & policies on their account and/or devices such as authentication strength, endpoint security aggression, etc. No personal interests (e.g. social media, etc) or external devices should be accessed/connected to devices in this category.
- Users of campus systems may not allow data to be outside of campus control without explicit permission from ITS. This includes but not limited to exports, data bridges, uploads, etc in addition to protecting credentials.

GENERAL RESTRICTIONS

- These computer privileges shall not be transferred or extended by the college's students, faculty, staff or administration without the written approval of the President and/or the President's designee.
- The user shall maintain considerate and ethical behavior in the use of college computer and network resources.
- The user shall not willfully create, copy, or disseminate computer viruses nor threaten to install or to infect the college's computer resources with any virus.
- Any unauthorized use, access, alteration, addition, destruction, duplication, or deletion of computer or network resources, or the information contained therein, is prohibited.
- The user shall avoid wasting computer resources by activities beyond the scope of legitimate administrative or instructional requirements.
- The user shall avoid the use of any mass email application or the utilization of on-campus mass email accounts unless authorized by ITS.
- The user shall be sensitive to the public nature of all computing facilities. All networks, network message traffic, and computer systems, including individual workstations, are subject to review for compliance with existing college policies.
- The user shall determine the licensing status of any software or data prior to copying or transferring the product.
- The user shall have prior written approval from the appropriate supervisor or administrator and Information Technology Services before installing on college computers or networks any software not provided by the college. The user shall be responsible for the registration and license compliance for any software not provided by the college. Only lawfully acquired software may be installed on college computers and networks.
- The user must ensure the integrity of all foreign software, physical media, or hardware before installing, or using such software, physical media or hardware on college computers or networks. "Integrity" in the context of this policy, includes assurance of compatibility with existing software, physical media, or hardware, as well as freedom from contamination by any type of computer virus. "Foreign" computer software, physical media, or hardware includes any computer software, physical media, or hardware which: (1) have not been provided by the college, or (2) have been removed from and then returned to the campus,

or (3) have been used on the campus in, or in connection with, any computer software, physical media or hardware not provided by the college.

- The user shall obtain, from the appropriate college authority, prior written approval for the planned installation and proposed applications of any type of computing 'server' device, or 'server' software. All information or material placed on any type of computer server device shall comply with all applicable college policies and practices and all laws governing the use of computer, network devices, and the Internet.
- The user shall access only those computing resources, and those accounts authorized by the appropriate college authority. The user must protect the integrity of personal files, personal data and personal passwords. The user shall respect the privacy of the college's and other users' resources.
- The user shall not attempt to sell any college-owned equipment.

Legitimate Use: Computer and network resources of Warren Wilson College are privileges provided solely for legitimate use by the following: students; faculty and staff; and authorized agents of the college performing activities for the benefit of or with respect to the instructional or administrative missions of the college. Computing and network resources include, but not limited to all forms of electronic and physical media and services provided by the college including computers, email, telephones, voicemail, fax machines, cellular services, online services, intranet, and Internet.

Legitimate uses of these computer and network resources are limited to: college-related instruction, independent study, research, and official work of college administration, staff, students, campus organizations and agencies of the college, and such other specific uses as are expressly authorized by the President and/or the President's designee. The computer and network resources may not be used for commercial or for-profit purposes without the written approval of the President and/or the President's designee.

Computer and network resources including but not limited to systems such as teleconferencing, chatting, online learning may not be used to store, transmit, or receive any text, image, audio, video, or other materials that are:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene, sexually explicit or pornographic;
- Defamatory or threatening;
- In violation of any license governing the use of software; or
- Illegal or contrary to Warren Wilson College's policy, business, or educational interests.

Ownership and Copyright: All college-provided computer resources are licensed from vendors or owned by the college. Users have no rights of ownership to these computer resources.

- Each user shall comply with all licensing agreements for college-provided software. Each user shall comply with all copyright laws.
- Each user shall comply with all relevant copyright laws as they pertain to any software, movie, music, art, and any other covered work. Downloading, storing, and transmitting any copyrighted work without a license is a violation of federal law and the user may be prosecuted by the copyright holder. If you need more information on copyright laws please visit http://copyright.gov/title17

Acquisition of College Technical Resources
All computer, network, audio-visual, software, and other technology related acquisitions and purchases, regardless of funding source (operating, capital, endowment, donation, etc), will be handled or approved by ITS. Individuals who do not order these items in consultation with ITS may have their college purchasing privileges revoked and/or

may not be reimbursed for the expenditure. This does not apply to students using personal funds for purchasing technology for their own personal use.

Data Backup and Management
All data stored on college-owned servers is backed up daily. Data stored on college owned desktop and laptop computers is not backed up. It is the responsibility of the user to backup their data utilizing Google Drive or other approved solutions. ITS will assist with the migration of work-related files only between college owned computers and bear no responsibility to manage or migrate personal data. Employees are encouraged to keep personal use of college-owned devices to a minimum.

Ownership of Technology and Account Management Practices
All computer and network resources provided by the College remain property of the College. All students, staff, faculty, and others who are provided these resources are expected to surrender them immediately upon separation from the college or at the termination of duties requiring these resources. All account access including e-mail is generally managed by the following rules but subject to change at any time at sole discretion of the institution:

- Staff separating from employment will have accounts closed immediately.
- Faculty in good standing upon separation from employment are granted 60 days of continued e-mail use to conclude research and scholarly relationships.
- Students who graduate will have a forward rule configured on their behalf such that email sent to their WWC address is forwarded to their personal email address on file with the College.
- Students on official leave of absence with the Registrar's Office will retain their accounts until their relationship with the College concludes either by withdrawing or by returning and graduating.
- Official retirees who request an e-mail account may be provided one with approval from HR and overseeing division officer. Compliance with all federal and state laws is still expected and required as is compliance with all other rules in this policy.

Students Living On-Campus
The college recognizes that students living on-campus will also utilize the college's Internet connectivity for personal use. While personal use is approved for students, compliance with all federal and state laws is still expected and required as is compliance with all student code of conduct rules.

- Copyright violations – Downloading software, movies, music, or other copyrighted materials is strictly prohibited unless the download of such material is provided by the copyright holder and/or an appropriate license for the use is granted to you. The word download is inclusive of any form of transmission such as streaming, whole file download, or partial file download (torrents, etc).
- Commercial and for-profit use – Commercial and for-profit use is strictly prohibited. This includes operating websites originating from a computer on-campus, web cam or chat services for pay from an on-campus computer, or other commercial or for-profit uses without the written permission of the President or the President's designee and the ITS office.

Enforcement
Violation of this policy may result in revocation of utilization privileges, administrative discipline, or immediate termination of the violator's relationship with the college and could lead to criminal and civil prosecution. The college is authorized by anyone utilizing its computer and network resources to cooperate with government and civil authorities in the prosecution of any criminal and civil matter against any person who violates this policy,

including disclosure of any records, information, data, images, communications, recordings, or other evidence in the custody of, or accessible by, the college.

Sensitive Data

In general, sensitive data refers to both non-public personally identifiable information (PII) as well as intellectual property of the institution. That is protecting the rights & privacy of our constituents as well as the organization itself. Examples include but not limited to PII such as social security numbers; credit card, banking, other financial information, restricted biographic data, grades, conduct & health records as well as institutional process, banking accounts, contracts, personnel files, closed meeting minutes, etc.

Warren Wilson College requires all users to adhere to FERPA, HIPAA, PCI, and other compliance standards. The above list is not exhaustive -when in doubt, inquire with ITS to determine if any of the data or systems you use is considered sensitive. Never publish or share without explicit approval.