PRESCOTT COLLEGE POLICY

TITLE: COMPUTING AND COMMUNICATIONS ACCEPTABLE AND RESPONSIBLE USE POLICY

APPLICABILITY

All Approved System Users: Students, Alumni, Staff, Faculty, Administrators, and guest users

POLICY

Prescott College provides a wide range of computing resources to support the educational mission and administration of the College. This policy establishes the boundaries and acceptable and responsible use of College's computing and communication resources, including computers, networks, electronic data, electronic mail services, electronic information services, electronic mail services, voice mail, telephone services, and other related computing facilities. This policy reflects the College's desire to promote free exchange of information between and among students, faculty, staff, and the global information community while respecting the principles of free speech and compliance to applicable communication laws.

College-owned computing equipment, networks, services, and resources are provided for the purpose of conducting College-related activities and are therefore considered College property. The College, as owner of such property, has the right to access information on the system stored, sent, created, or received by students, alumni, faculty, or staff including electronic mail, as it deems necessary and appropriate. While the College values the importance of individual privacy and endeavors to balance that value against the needs for institutional security and for compliance with legal and institutional standards that allow the College to provide campus-wide support, individual users should not expect privacy when using shared information systems.

Users are obligated to protect College computing systems from illegal or damaging actions, either knowingly or unknowingly. This policy provides description of unacceptable uses of College computing resources and how to report violations; however, the College may at any time make determinations that particular uses are and are not appropriate.

Use of Prescott College Information Technology resources, including the network, is considered an agreement to abide by this policy.

PROCEDURES

1. **Use of information technology resources is limited to research, instructional, or administrative purposes only.** Computing resources may not be used for commercial purposes or personal gain. Use of computer services for any commercial purpose, partisan political purpose, personal undertaking, or for any unlawful purpose is prohibited.

2. **Users must uphold laws and ethics while using Prescott College computing resources.**
    - Comply with laws governing copyrighted materials. Making, distributing, storing, or using unauthorized duplicates of copyrighted material, including software applications, proprietary data, and information technology resources is prohibited. Section No. IX Policy No. 905.0 Page 1of 2 Responsible Executive: Provost Responsible Office: Information Technology Effective date:

07-01-98 Revision date: 06-03-00; 9-21-06; 01-02-12 2 This includes illegal file sharing of entertainment (e.g. music, movies, and video games) files in violation of copyright laws.

- Borrowing, lending, falsifying, allowing, or facilitating the unauthorized access to use of College computing resources by a third party is prohibited. This includes violating the terms and conditions of software license agreements for software distributed by the College by giving, lending, selling, or leasing such media or software to others for their own use. Users should assume that all College supported software is proprietary and may not be copied.
- Using College computing resources to gain or attempt to gain unauthorized access to computing resources either inside or outside of the College is prohibited, including obtaining user IDs and/or password(s) or impersonating another person on a computing resource.
- Using electronic media to harass or threaten other persons, or to display, design, copy, store, draw, print, or publish obscene language or graphics is prohibited.
- Intercepting or attempting to intercept or otherwise monitor any communications not explicitly intended for the user, without authorization, is prohibited.
- Copying, reading, accessing, using, misappropriating, altering, publishing, or destroying computer files, data, documents, or other files of another individual or attempts to do so, without the permission of that individual or authorized administrator is prohibited.
- Users must follow all Prescott College policies, including but not limited to communications, marketing and publishing regulations when utilizing computing resources.

3. Users must participate in computing security measures of the College.

- Users shall protect computing credentials, and never share passwords with others, including IT personnel.
- Users should not use removable storage devices (such as thumb drives, jump drives, USB remote storage devices, portable caddies, SD storage, CDs, DVDs, etc) on the Prescott College system due to the security risk they pose.
- Users shall relinquish college-issued computing equipment for the purpose of required repairs and security measures.
- College network systems and devices are regularly scanned for security purposes. Attempting to circumvent or subvert system or network security measures is prohibited.
- Creating or propagating malware or viruses is explicitly prohibited.

4. Users must protect the functionality of the College's IT systems.

- Intentionally or recklessly abusing, monopolizing, or misusing computing resources which cause damage, system interruptions, resource degradation, or harassment to other persons is prohibited.
- Actions or attempted actions that degrade or disrupt resource performance, security, or administration operation including, but not limited to, intentionally introduction any computer virus or similar disruptive force into any computer resource is prohibited.
- Repeatedly or purposefully engaging in activities which can be reasonably expect to, or do, unreasonably tax computing resources or go beyond their intended or acceptable use is prohibited.
- Attempting to alter the Prescott College computing infrastructure is prohibited. Users must not install or alter wiring, or extend or retransmit the network, or connect any computing or

networking components (including, but not limited to, bridges, routers, DHCP servers, wireless access points, and hubs) on the College network without prior approval is prohibited.

5. Users with authorized access to internal College data have additional duties.

- Users who have a role that includes access to student information must protect the student information. Records containing information directly related to a student are confidential and protected from public disclosure by the Family Education Rights and Privacy Act. Employees must access only information to which they have been given authorized access or is publicly available, and may not disclose or distribute student information in a manner inconsistent with federal and state law and College regulations.
- All legally restricted, regulated and confidential information must be kept secure. Current best security practices are to be utilized when sending or receiving this data including encryption, authentication and, when away from campus, via a Virtual desktops. Employees may not forward such information to personal email accounts, nor store or transport restricted and confidential data on removable storage devices. Any exceptions shall be documented and approved by the Chief Operating Officer or their designee.
- Employees are to consult Information Technology and Institutional Research before integrating data.
- Employees in certain roles, such as Information Technology personnel, those with access to health or financial records, those who create new identities within the system, and users of specialized hardware, software, databases, or data must follow all computing training and protocols provided for their roles.
- Employees in supervisory roles are responsible for ensuring supervisees have the appropriate training for their role related to what type of data the employee accesses and any protocols that are required.

6. Violations of this policy should be reported immediately to Student Life, Human Resources, or the Office of the Provost. Violations of this policy will result in appropriate disciplinary action, which may include loss of computing privileges, suspension, termination, expulsion from the College, and/or legal action.