COMPUTER RESOURCES AND ACCEPTABLE USE

Computing Services:

Computing resources are available to support the academic and administrative activities of Temple College. Computer resources are not to be used for personal or commercial financial gain. This policy applies to any and all school computing resources, including, but not limited to, all Temple College owned computers, printers, other hardware, and licensed software.

Computer Security:

1. Unauthorized Use of Computer Accounts or System Access
    a. Unauthorized use of Temple College computers or unauthorized access to stored data, or dissemination of passwords or other confidential information to gain access to a computer system or data is in violation of criminal law (Computer Crimes, Section 33, Texas Penal Code) and can be a Class B or Class A Misdemeanor or a Felony of the third degree.
    b. Alteration, destruction, or false entry of data that impairs its validity, legibility or availability of any record maintained by Temple College is a violation of Tampering with a Governmental Record (Section 37, Texas Penal Code), a Class A Misdemeanor.
    c. Use of computer accounts for purposes other than those intended by the funding source, in particular, the use of departmental accounts funded by Temple College for the purposes of private gain or for other than instruction and research can be regarded as a misuse of funds.
    d. Regardless of the purpose or the intent of the unauthorized access, Temple College will recommend the filing of appropriate legal action as warranted.
2. Unauthorized Viewing or Changing of Data and "Computer Viruses"
    a. In the case of administrative data, only authorized users are permitted to have access to the data. "Browsing" of data by unauthorized users may be a violation of federal, state, and/or college regulations.
    b. Unauthorized access of another person's educational records to view that person's files without an educational need to know or proper authority is a violation of the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).
    c. Unauthorized changing of data is a violation of the State Penal Code, and such actions will be prosecuted. This statement covers all administrative systems on campus, including the Student Information System.

Board Approval Date: January 28, 2013
Effective Date: January 2, 2013
Final Revision Date: September 28, 2012
Policy Manual Review Committee: March 9, 2017

d. Intentional creating or spreading of a "computer virus" or other malware is considered to be unauthorized changing of data and is a violation of the State Penal Code, and such actions will be prosecuted.

3. Password Protection
   a. All College employees and students will be provided a username and password that permits access to the Temple College network for conducting official business and academic coursework. At no time will the user provide access to his/her account by providing someone else their login information (username and password). It is an offense under the Computer Crimes, Section 33, Texas Penal Code to access or attempt to gain access to a computer system or computer material to which one is not entitled.
   b. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe/locking cabinet if in hardcopy format or in an encrypted/password protected file if in electronic format.
   c. Passwords are not to be transmitted electronically over the unprotected Internet, such as via email. Do not use the “Remember Password” feature of programs on your computer.
   d. Computers or other computing devices must not be left unattended without enabling a password-protected screensaver or logging off the device.
   e. If your password is known to others, change it immediately and notify the Information Technology Help Desk.
4. Portable Devices & Cloud Storage
   a. Portable devices include, but are not limited to laptops, notebooks, tablets, flash (thumb) drives, memory cards, portable hard drives, PDAs, Smart phones and any other emerging technology that contain a processor and/or memory for storage of data.
   b. Employees using portable devices must exercise care to safeguard their devices and any confidential data contained on the device.
   c. All portable devices used for College business that contain confidential information must have password functionality enabled and encryption installed and enabled.
   d. When a user saves information in public cloud storage, Temple College cannot guarantee appropriate technical and administrative access controls for the data. Public cloud storage of confidential information, such as but not limited to, student record data, personnel data, financial data (budget and payroll), student life data, departmental administrative data, legal files, research data, proprietary data, and all other data that pertains to, or supports the administration of the College is not permitted.
5. Unauthorized Copying of Software or Data

a. All commercial software and data are covered by a copyright of some form. Duplication of software and/or data covered by such copyrights is a violation of the copyright law. Students, faculty, and staff must observe contractual terms for computer software packages used at Temple College. Software products are for educational purposes only and may be used only on college computers. Software (or documentation) may not be copied, disassembled or decompiled.

6. Unacceptable Usage
   a. Unacceptable computer usage includes, but is not limited to the following:
      i. Logging on or attempting to log on with a username other than your own.
      ii. Logging on with your account and allowing others free use of your computer while logged into the campus network.
      iii. Copying, installing, or using any software or data files that violate a copyright or license agreement.
      iv. Sending, sharing, or storing mail, files, messages, etc. that contain:
         1. profanity, obscenities, or other language of an inflammatory nature, exceptions for instructional purposes;
         2. information which infringes upon the rights of another person;
         3. information which may threaten or injure someone else such as cyberstalking, cyberharassment, and/or cyberbullying;
         4. files or information covered under the Digital Millennium Copyright Act unless permission has been obtained from the owner(s).
      v. Employing an internet browser (Internet Explorer, Firefox, Chrome, etc.) on a campus computer for the sole purpose of surfing the Internet in search of pornographic sites, illegal gambling sites, terrorist sites, or other similar, questionable sites.
      vi. Using computing and/or network resources to gain unauthorized access to remote computers; using computing and/or network resources to launch Denial of Service attacks, broadcast attacks, mail-bombing, packet-flooding or overloading any system located on or off the premises.
      vii. Using computing resources to harass others by sending threatening, libelous, or sexually, racially, or religiously offensive messages.
      viii. Using computer resources to develop, perform, and/or perpetuate any unlawful act or to improperly disclose confidential information.