Electronic Resources Acceptable Use Policies

All persons who have been granted use of Austin College's information resources must comply with all College policies and applicable laws regarding the acceptable use and protection of College information resources. This specifically means adhering to the policies listed below. Failure to do so could result in the loss or compromise of private and/or sensitive College and individual information and/or the degradation of information systems.

Purpose

The purpose of these policies is to ensure the availability, protection, and proper use of College electronic information and systems to meet the needs of all campus community members and protect sensitive data of all College constituencies.

Scope

- All students, faculty, staff, and others,
- using any Austin College electronic information resource, whether individually controlled or shared, stand-alone or networked,
- including all network elements, personal computers and other electronic devices, workstations, servers, associated peripherals, audio-visual equipment and software.

Individual Policies

Information Resources available for your use

- electronic devices for which you are specifically authorized.
- all computers that are located in WCC open areas, residence hall computer labs, and those academic and library computer labs which are not restricted to specific classes or groups.
- You should not access network drives and other College information locations for which you are not specifically authorized.

Ownership and Sharing of Information and Data

- All data and information generated on College-owned computers and electronic devices during the process of performing an assigned job responsibility are considered to be owned by the College, and may be accessed by the College.
- All data contained in email messages which reside in the College's email system, whether generated through College-owned computers or not, are deemed accessible by the College when necessary.
- You should comply with applicable laws, college regulations, and department rules concerning the sharing of data and information intended for limited access
    - Laws include those related to **FERPA** and **HIPAA**
    - Sections JP5, JP6, JP9, PP4, PP6, and OP1 of the College **Operational Guide** [intranet]
    - Department rules communicated to department employees and student workers

When in doubt, please don't share the information.

- This also includes complying with campus norms related to the privacy of personal information, whether deemed "sensitive" or not.

The College does not exist in isolation from other communities and jurisdictions and their laws. As a result of investigations, subpoena or lawsuits, the College may be required by law to share information with appropriate authorities.

Equipment Configuration Protection

Users of College-owned electronic hardware and software should not modify, or attempt to modify, the configurations of those resources unless specifically authorized to do so by IT personnel.

This specifically applies to:

- Attempting to reconfigure College-owned electronic hardware, software, cabling, or accessories in teaching spaces, meeting rooms, and other campus venues in which electronic equipment is being used that is NOT specifically assigned to you.
- Attempting to repair any College-owned or IT-supported electronic hardware, software, cabling, or accessories without consulting IT and without specific authorization to do so.

This does NOT apply to:

- Minor hardware and software configurations that are widely understood to be normally made by end-users on single-user devices assigned to them (such as power energy settings, browser preferences, printer mappings, etc.).

- Configuration changes specifically authorized by IT personnel on a one-time basis to aid in quickly resolving a hardware or software problem being experienced by an end-user.

Copyrights

All copyrighted materials must not be copied except as specifically allowed by the copyright owner or otherwise permitted by copyright law.   Copied material must be properly attributed. Computer and communications information that is plagiarized is subject to the same sanctions as that of any other medium.

Software Licensing

- You must request a legitimate copy of a specific software program if the license does not permit free distribution or use of the software (freeware, open source, etc).
- Do not copy any piece of software you did not create unless you have determined you will not be in violation of a software license or other intellectual property provision.

Information Security

- Defects discovered in a system's security must be reported to the IT Help Desk or IT Executive Director as soon as possible, ideally within one hour of discovery, in order to be resolved quickly.
- Attempts to circumvent the security of information resources in order to gain unauthorized access to a system or to another person's information are prohibited and may violate applicable laws.

Wireless Devices

- All devices which authorized end-users wish to have access to the College wireless network must be registered through IT before access is granted. Any device which IT determines causes interference with or degradation of the wireless network will not be approved for connection.
- Any personal device that broadcasts a wireless network or wireless traffic on standard wireless radio frequencies is prohibited from operation anywhere within the campus perimeter. This includes, but is not limited to, wireless routers or access points, certain wireless printers, cellular mobile hot spots, personal media players, and other devices that allow direct wireless connections.
- Attempting to manipulate the wireless network, electronically or physically, to change the performance or signal strength is prohibited.
- Intentionally intercepting or attempting to decrypt wireless signals intended for another user or device is prohibited. This includes the use of tools or programs that "sniff" or monitor other users' wireless traffic.

Proper use of Information

- College information resources should be used for appropriate College functions, and may not be used for profit-making enterprises of any type unless specifically authorized by a College officer.
- Sending fraudulent, harassing, obscene, threatening or other messages in violation of applicable federal, state or other law or College policy through electronic communication facilities is prohibited.

Consequences of Violations

Violation of these policies may subject a person to disciplinary review and could result in the loss of information resource privileges and/or other disciplinary actions as stated in sections JP5 and OP1 of the OP Guide.

Requests for more information should be addressed to the Executive Director of Information Technology.