# Student/Guest Acceptable Use Policy

## Acceptable Use Guidelines

These guidelines are intended as a minimum set of standards to assist in the interpretation and administration of policy.

Student/Guest shall use computing and information technology resources only for their intended purpose.
For example: it is a violation

    A. to upload, download, or distribute pornography;
    B. to use privileged access for other than intended use;
    C. to use former privileges after intended usage timeline has expired.

Student/Guest shall protect the access and integrity of computing and information technology resources.
For example: it is a violation

    A. to intentionally release a virus or worm that damages or harms a system or network;
    B. to prevent others from accessing an authorized service;
    C. to attempt to deliberately degrade performance or deny service;
    D. to alter or destroy information without authorization.

Student/Guest shall use only those computing and information technology resources for which they have authorization.
For example: it is a violation

    A. to use unauthorized  resources;
    B. to access files, data, or processes without authorization;
    C. to use someone else's account and password or share your account and password with someone else;
    D. to purposely look for or exploit security flaws to gain system or data access.

Student/Guest shall abide by applicable laws including, but not limited to, copyright, intellectual property rights, and licensed software

For example: it is a violation

    A. to download, use, or distribute pirated software, music, or movies;
    B. to upload, download, distribute, or possess child pornography;
    C. to post information protected by the *Family and Educational Rights Privacy Act* (FERPA).

Student/Guest shall respect the privacy and personal rights of others.
For example: it is a violation

    A. to tap a phone line or run a network sniffer;
    B. to access or copy another user's e-mail, data, programs, or other files;
    C. to post or share incriminating information or inappropriate media.

## External Devices

The College shall not be responsible for any damage caused to personal devices including, but not limited to, external hard drives, zip drives, CD drives, cameras, memory, printers, and smart phones, that are connected to College owned computers or other devices. Student/Guest who uses external devices does so at their own risk.

## Software

All software installed on College computers is licensed for use on College workstations only. This software shall not be copied to disk or otherwise transferred and installed to personal computers.

Student/Guest shall not install software on College workstations either by downloading or from external media. Software authorized by a supervisory Vice President shall be installed on College computers by IT Department personnel.

## File Sharing and Copyright Violations

Illegal file sharing and copyright violations shall not be allowed. An investigation shall be initiated upon receipt of a reputable claim of illegal file sharing or copyright infringement. If there is evidence that illegal file sharing or copyright violations have occurred, access to network services shall be terminated until the suspected violator meets with the Vice President of Student Success. If the Vice President of Student Success determines a violation has occurred, the student/guest shall be subject to disciplinary procedures up to and including removal from campus.

Violators may also be subject to civil and criminal punishment. The College shall cooperate with criminal investigations related to illegal file sharing or copyright infringements.

## Security Camera

Security cameras are installed to deter and identify criminal activity.  Use of security cameras shall not violate established privacy laws.

Information obtained from the cameras shall be used exclusively for policy and/or law enforcement.

Any activity that disables, obstructs or alters the view of installed cameras shall result in disciplinary action up to and including removal from campus.

## Copy/Print

Student/Guest using the printers and copiers on campus shall only print using their authorized account(s).  Printing should only be done as it relates to the purpose of being on campus.

## Email

Email is one of the main communication tools used to communicate with a student. Students are encouraged to use a frequently used personal email account for this purpose.

A college student email account is provided for currently enrolled student on request. The account is the responsibility of the user, who shall be accountable for any unauthorized use thereof.

Inappropriate use of College issued student email account shall result in disciplinary action up to and including removal from campus.  Inappropriate use shall include but shall not be limited to:

     A.  Violations of College policies and procedures
     B.  SPAM
     C.  Downloading or distributing pornography
     D.  Harassment
     E.  Personal subscriptions (e.g. daily jokes, daily trivia, daily horoscopes, sweepstakes entries, vacation information, etc.)
     F.  Initiating or forwarding chain letters
     G.  Promoting personal business

Student/Guest receiving suspicious emails may refer to the IT Department.

## Telephone

College telephones are provided for business use.

Residences Hall occupants have access to an analog line with voice mail in the assigned room. Occupants must supply their own analog phone. The External Devices section in

this document applies to the Student/Guest supplied phone.  Dial a 9 to get an outside line. Local calls are free and the Student/Guest is encouraged to use a calling card for long-distance calls.

## Internet

Access to the internet is intended to allow electronic communication, research, and browsing for College related matters. Personal use is allowed as long as it does not affect system performance.

## Password

All Student/Guest who have access to the College network shall adhere to the password procedures as defined in the Technology Plan. The proper use of passwords shall be the responsibility of the user, who shall be accountable for any unauthorized use thereof.

## Banner Self-Service

Due to the sensitive nature of information in Banner Self-Service, sessions shall automatically disconnect after 30 minutes of idle time. Users shall keep logon/pin information secure at all times.

## Cooperation with IT Personnel

Activities which interfere with the operation of any IT systems, even though not explicitly prohibited by this document, shall be immediately discontinued by the IT department until fully investigated and resolved.  Failure to comply shall result in disciplinary action up to and including removal from campus.

### Miles Community College Acceptable Use Policy

After reading the Miles Community College Acceptable Use Policy, I understand and will abide by the policy.  I further understand that any violation of the Acceptable Use Policy is unethical and may constitute a criminal offense.  Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.