COMPUTER USE POLICY

The purpose of this policy is to promote the use of the University's and student's computing resources in an efficient, ethical, and lawful manner and to provide an overview of the uses of University computing resources. It is intended as an addition to existing University policies concerning academic honesty, intellectual property, use of copyrighted materials, the usage of facilities and policies prohibiting harassment, unlawful discrimination, sexual misconduct, and other unprofessional conduct.

Additional relevant computer/email/Wi-Fi use documents are found on the technology tab of the portal (https://my.ketchum.edu/ICS/Students/Free-form_Content.jnz).

1. Appropriate Use

The University's computer resources support its instructional, research, and administrative activities. Appropriate use should always be legal, ethical, reflect academic honesty, reflect community standards, and show restraint in the consumption of shared resources. Use should demonstrate respect for intellectual property, ownership of data, system security mechanisms, and individual rights and freedoms.

Access to the University's computing facilities is a privilege and the University reserves the right to limit, restrict, or extend computing privileges and access to its resources.

The student's computer resources should meet the University standards described in the Recommended Computer Standards for Students document found on this Portal link (https://my.ketchum.edu/ICS/New_Students/Frequently_Asked_Questions.jnz?portlet=Helpful_Documents). Laptops or mobile devices should have strong passwords and/or complex unlocking patterns to access the device. Security patches announced by device manufacturers should be installed immediately after each release. Anti-virus/Anti-malware software should be installed and regularly updated. Patient data must never be stored on a student's personal computing devices.

2. Confidentiality & Privacy

In general, the University treats information stored on computers as private. However, there is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment. Email and data stored on the University's network of computers may be accessed by the University for a variety of business-related purposes. To the greatest extent possible, individuals' privacy should be preserved. Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form may not be secured and may be vulnerable to unauthorized access and modification by third parties.

3. Prohibited Use

Examples of misuse include, but are not limited to:

- using an unauthorized computer;
- installing personal software on University computer systems;
- obtaining a password for an account without the consent of the account owner;
- using the campus network to gain unauthorized access to any system(s);
- knowingly performing an act that may interfere with normal computer operations;
- knowingly running or installing a program intended to damage the system;
- attempting to circumvent data protection schemes or uncover security loopholes;
- violating terms of licensing agreements or other laws;
- using email, social media, or other networks to harass others;
- masking the identity of an account or machine;
- posting anything on the internet that violates existing laws or the Student Code of Conduct; **and/or**
- attempting to monitor or tamper with another user's files.

Every time a site on the internet is accessed or communication happens via e-mail, your e-mail address, which identifies the University, is recorded. Using any computer system in any way to discredit the University or compromise University confidential or proprietary information is prohibited.

All violations or alleged violations by students should be referred to University Conduct for adjudication. Additionally, misuse can be prosecuted under applicable law.

4. E-Mail & Communications Policy

MBKU and its Programs maintain a direct and open line of communication with all students to ensure access to information. MBKU provides a University email account for all students upon enrollment. This address is used by all entities on campus for communicating with students. Students are expected to review and respond to email daily. Email sent to University accounts is assumed to be read. Students sending emails on University business should use their provided University email account. Personal communications using MBKU email systems should be kept at a minimum.

The email address naming convention is the following:

a. **Employees**: <first initial of first name><full last name>@ketchum.edu (e.g., Jane Smith would be jsmith@ketchum.edu). When a conflict occurs, additional characters of the first name will be used (and then middle name, if necessary).
b. **Students**: <full first name><full last name>.<SCCO/SPAS/COP><2 digit graduating year>@ketchum.edu (e.g., Jane Smith in OD class of 2025 would be janesmith.SCCO25@ketchum.edu). This format will begin with the fall 2021 incoming students. Previous students do not have program designation **or** have program short-hand designation (OD/PA/PH).
    - If two students have the same name and are in the same program and graduating class, their middle initial will be added to both addresses (e.g., JaneAsmith.SCCO25@ketchum.edu and JaneLsmith.SCCO25@ketchum.edu).
    - If two students have the same **full name** and are in the same program and graduating class, the students will be asked if they have a nickname. The nickname will be used in place of the first name and listed on the MBKU Directory.
    - Student email groups are available to facilitate group conversations. The format of student email groups are as follows: <SCCO/SPAS/COP>classof<graduating year> (e.g., SCCOclassof2025@ketchum.edu for the graduating class of 2025 for SCCO).

- The following email naming convention applies to MBKU's Non-Degree, Eulji, and MSVS programs.
  - COP Non-degree: <full first name> <full last name>.ND@ketchum.edu
  - Eulji International: <full first name> <full last name>.EULJI@ketchum.edu
  - MS in Vision Science: <full first name> <full last name>.MSVS@ketchum.edu

5. Reporting a Cyber Incident

The following cyber security incidents should be reported to ITSupport@ketchum.edu as quickly as possible so that the University may take appropriate action to minimize any negative impact.

Types of Incidents

- Clicking on a phishing email
- If you suspect your computer has been infected with malware
- Unauthorized disclosure of ePHI (Personal Health Information) whether accidentally or not

The University counts on all of us to "Say something if you see something" that appears to be a cyber security incident.

All students should immediately change the temporary password to a personalized password. Due to the importance of passwords in safeguarding University information, strong complex passwords are required. A strong complex password has the following characteristics: at least 8 characters long, with upper- and lowercase alpha characters mixed with symbols and numbers. Please keep in mind your email password expires every 12 months. It is recommended you change it before it expires to avoid loss of access to your account. Your email password is also your Moodle, Library Resource, and Wi-Fi password.

All electronic messages maintained on MBKU platforms are the property of MBKU. Users should not have an expectation of privacy. Access may be denied when there is a substantiated reason to believe that violations of policy or law have occurred or, in time-sensitive cases, when required to meet critical operational needs. The administrators of the University e-mail facility may, within certain limits, block mail including external, unsolicited, bulk e-mail or "spam."

Users should not assume the privacy of their e-mail. Users are advised not to send confidential University communications via e-mail. E-mail may be subject to disclosure under law. Backup copies may be retained for periods of time even if the user has deleted the message from the account. During routine system maintenance, troubleshooting and mail delivery problem resolution, network or systems staff may inadvertently see the content of e-mail messages.

Students should set up a signature line in their email. Students may not describe themselves as a candidate for their degree. The term "candidate" is reserved for students who have completed all their coursework, apart from their dissertation. The following is an example of a signature line for student use:

First Name Last Name
Optometric Intern / PA-S / Student Pharmacist
Class of 20##
Southern California College of Optometry/School of PA Studies/College of Pharmacy
Marshall B. Ketchum University

Student email addresses will be kept indefinitely, even after graduation. It will become a forwarding-only email address that directs to a designated external email account. Students must maintain an active external email address and update MBKU whenever that changes. Please see the Student Address Update Form on this Link to Portal (https://my.ketchum.edu/ICS/Online_Forms/). After graduation, contact University Advancement/Alumni Relations to update the external email address. The email group for each class year (i.e., SCCOclassof2025@ketchum.edu) will also be kept indefinitely to facilitate future communications.

Creation of non-individual email addresses (aka shared mailboxes or distribution lists) needs to be approved by the Director of Information Technology. Additionally, there are use restrictions on certain distribution groups. The following groups are restricted to the President's Executive Council (PEC), department heads and specific designees for official University business only:

- Everyone (includes students, employees, residents)
- All Employees
- Admin
- Ketchum Health (includes Employees and Residents of Ketchum Health)
- Clinic (includes Ketchum Health and UECLA)
- All Faculty
- All Staff

Unacceptable Usage of Emails:

- Emails containing confidential information such as social security numbers and credit card information.
- Sending or forwarding emails with any libelous, defamatory, offensive, racist, or obscene remarks.
- Copying and sending written material that is subject to copyright protection without permission.
- Knowingly sending an attachment that contains a virus.
- Sending unsolicited email messages.
- Forging or attempting to forge email messages.
- Disguising or attempting to disguise your identity when sending email.
- Sending email messages using another person's email account without their consent.
- Copying a message or attachment belonging to another user without permission of the originator.
- Sending chain letters or junk emails. Mass emails require approval from IT.

6. Social Media Standards

MBKU has created these social media guidelines to assist students in making professional decisions. The permanence and written nature of online postings cause them to be subject to high levels of scrutiny. Therefore, postings within social networking sites are subject to the same standards of professionalism as any other personal or professional interaction and are treated as if made in a public forum. This is the case for students, faculty, staff, and all other MBKU constituents.

The following are MBKU's expectations regarding social media participation. While not all-inclusive, it is expected that students use the highest integrity and judgment when engaging in any communication.

a. Monitor other people's statements/photos, etc. that may be viewed under your name. If others are displaying unprofessional behavior, consider changing your restrictions to avoid those statements, etc. from being affiliated with you.
b. Inappropriate postings may be considered as violations of the Student Code of Conduct (https://catalog.ketchum.edu/university-student-handbook/student-conduct/).
c. Always avoid giving medical advice on social media, as this may result in a violation of HIPAA and may cause danger to others.
d. Never discuss specific patient information online, even if all identifying information is excluded. It is possible that someone could recognize the patient to which you are referring based upon the context.
e. Under no circumstances should photos of patients or photos depicting the body parts of patients be displayed online. Once you post, the actions of others could lead to legal or professional consequences.
f. To maintain healthy patient-clinician relations and to avoid potential legal consequences, refrain from interactions with patients on social media platforms.
g. The lines between public and private as well as personal and professional are often blurred online. By identifying yourself as a MBKU student, you may influence perceptions about MBKU or your program by those who have access to your information. All content associated with you should be consistent with MBKU's values and professional standards.
h. Influencer-driven content is very popular. As a student, if you are approached to be an influencer and represent yourself as an MBKU student, permission must be approved by Enrollment and Student Services and Marketing and Communication Departments prior to any content being created.
i. Final approval of content posted on MBKU's official social media accounts, including Instagram, Tim Tok, LinkedIn, and Facebook must be approved by the Marketing and Communications Department.