Southwestern Michigan College Board Policy – Use of College Technology Resources

Last Reviewed	Last Updated	Effective Date
08/17/2020	08/17/2020	08/17/2020

DIVISION I – GENERAL

I.31 USE OF COLLEGE TECHNOLOGY RESOURCES

This policy governs the use of technology at Southwestern Michigan College including but not limited to hardware, software, systems, networks, data stored, transmitted or accessed using College computers, tablets and College provided access to email, Intranet, and Internet related services.

Southwestern Michigan College encourages the use and application of information technologies to suppmt the educational and community service mission of the institution. SMC's Technology Resources can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

DEFINITIONS
Technology Resources: Including, but not limited to, hardware, computer and telephone equipment (including cell phones owned by the College), laptops, desktops and tablets, electronic files and communication, email traffic, email lists, listservs, software, systems, networks, data stored, transmitted or accessed using College computers and College provided access to e-mail, Intranet, Internet, World Wide Web, or any other internal or external service, server or provider.

Users: Faculty, Staff, Students, Pattners, Visitors

Acceptable use terms and conditions:

- The primary purpose of electronic systems and communications resources is for College-related activities only.
- Users do not own accounts on College owned technology equipment, but are granted the privilege of exclusive use. Users may not share their accounts with others, and must keep account passwords confidential.
- Each account granted on a Technology system is the responsibility of the individual who applies for the account. Groups seeking accounts must select an individual with responsibility for accounts that represent groups.

- The College cannot guarantee that messages or files are private. The College may monitor and record usage and content of all Technology Resources to enforce its policies and may use information gained in this way in disciplinary and criminal proceedings. Users of Technology Resources have no expectation of personal privacy in their use of or communication and information that is created, transmitted or stored using Technology Resources.
- Users must adhere strictly to licensing agreements and copyright laws that govern all material accessed or stored using SMC provided Technology Resources.
- When accessing remote systems from SMC Technology Resources, users are responsible for obeying the policies set forth herein as well as the policies of other organizations.

Conduct which violates this policy includes, but is not limited to the following:

- Unauthorized attempts to view, tamper with, delete, destroy, copy and/or use another person's accounts, computer files, programs, or data.
- Using SMC Technology Resources and/or accounts to gain unauthorized access to College systems or other systems.
- Using SMC Technology Resources for threat of imminent physical harm, sexual or other harassment, stalking, forgery, fraud, generally offensive conduct, or any criminal activity prohibited by Michigan or federal law.
- Attempting to degrade performance of SMC Technology Resources.
- Attempting to deprive other users of access to SMC Technology Resources needed to perform assigned business or educational functions.
- Using SMC Technology Resources for commercial activity such as creating, promoting, marketing, or selling products or services.
- Copying, storing, sharing, installing, downloading, uploading, or distributing software, photographs or depictions, screensavers, applications, programs, games, movies, music, and other materials currently without prior written autorization from the Office of Information Technology (OIT) or that is protected by copyright, except as permitted by licensing agreements or fair use laws.
- Sending or receiving material of a profane, prographic, or threatening nature.
- Sabotage, misuse or abuse of equipment or software on or off campus, through the introduction of viruses or mechanical tampering.
- Plagiarizing, altering or tampering with the work of others.
- Unauthorized junk mail, mass e-mailings to newsgroups, mailing lists, or individuals, i.e. "spamming" or propatating electonic chain letters.
- Unauthorized "broadcasting" of unsolicited mail, material, or information using College computers/networks.
- Transferring, deleting, destroying, or tampering with data, documents, information or material created, transmitted, or stored on Technology Resources in order to obstruct or mislead any investigation being conducted by the College or a law enforcement agency.
- Falsely assuming another person's or entity's identity or role without prior written authorization, or communicating or acting under the name, email address, or any other form of identification attached to a specific person, organization, or entity without prior written authorization.
- Creating or intentionally uploading, downloading or sending viruses, malware, spy ware, worms or other harmful programs or files.

- Circumventing or bypassing security measures or protocols in place to ensure the confidentiality, security, operation, integrity, and availability of Technology Resources.
- Campaigning for or against any ballot matter, political cause or campaign, legislative or regulatory actions, candidate for office or to conduct or support a political campaign or issue, except as may be authorized in writing or conducted by the College President in Federal, State and local matters concerning SMC students or operations.
- Creating the appearance that the College endorses, is affiliated with, or otherwise supports any organization, product, service, political candidate, or position on any matter of public concern.
- Creating, maintaining, sending, or distributing any information that is false or defamatory or invades the privacy of any individual, business, organization, or other entity.

Additionally, the College also prohibits the removal or relocation of designated stationary equipment (such as but not limited to desktop computers, monitors, desktop printers and copiers) or College provided software without prior written authorization by the applicable Cabinet member and correspondence to the OIT.

It is the desire of SMC to see that its Technology Resources are put to the best and most efficient use. SMC, therefore, requires that:

1. Users receive appropriate training in hardware and software use (or demonstrate proficiency).
2. Users be mindful of the time spent (as in "surfing the net") on machines, or materials consumed

The College acknowledges that occasionally employees use College Technology Resources assigned to them or to which they are granted access for non-commercial, personal use. Such occasional noncommercial uses are permitted by employees if they are not excessive; do not incur costs; do not interfere with the efficient operation of the College, its employees, or its computing resources; are not prohibited by the supervisor or faculty; and are not otherwise prohibited by this policy or any other College policy or directive.

The College will not provide technical support for any use not directly related to College business. Technology Resources may not be used for any purpose which is illegal, immoral, unethical, academically dishonest as in plagiarizing or cheating, damaging to the reputation of the College, inconsistent with the mission of the College, or likely to subject the College to liability as determined solely by the College.