

	POLICY	Motion No.	FF 1009-2023
	Acceptable Use of Information Technology Resources	Effective Date	04/18/2023
		Responsible Department	Information Technology
		Attorney Review / Date	NA

Pennsylvania Highlands Community College Information Technology (IT) resources are to be used for college-related purposes. Some examples of IT resources are computers, software, networks, and mobile devices. This policy applies to all users of College IT resources, whether affiliated with the College or not, and to all users of those resources, whether on campus or from remote locations. Users include staff, faculty, students, guests/visitors, and vendors.

The following conditions exist for any users of College IT resources:

1. Users of College provided hardware, software and/or the network are prohibited from accessing, communicating, publishing, displaying, or posting any slanderous or libelous material. For students and employees, exceptions may be made if the purpose of such activity is to conduct work-related research or is used in the auspices of teaching and/or learning directly related to College work.
2. All employees who store and/or process College-related information using hardware or software hosted or maintained by entities outside of the College (cloud computing) must only use College approved and/or contracted cloud services and applications for such activities.
3. Use of any College IT resources is an acknowledgment that the user may receive or be exposed to content, goods or services that the user may consider to be improper, inaccurate, misleading, defamatory, obscene or otherwise offensive and constitutes an agreement that the College is not liable for any action or inaction with respect to any such content on the Internet accessible through the College IT resources. In addition, the College is not responsible to the user for any content provided by third parties through the College IT resources.
4. Users of College IT resources must comply with all applicable legal requirements.
5. Users are responsible for the use of their individual College account and must take all reasonable precautions to prevent others from being able to access or use their account. Under no conditions should a user provide his/her credentials or allow another user to share their account.
6. Users shall not use IT resources to gain unauthorized access to College or external organization systems or networks.
7. Users must not knowingly post, transmit, re-post or re-transmit information that, if acted upon, could spread a virus, cause damage, or create a danger of disruption.
8. Recreational and personal use of the network is permitted; however, users should limit use of College IT resources for commercial or profit-making purposes.
9. The College reserves the right to configure the network in favor of the academic and operational mission of the College and does not guarantee that all devices will be able to connect to or operate with the network.
10. Users may not make unauthorized changes to the hardware or system-level software that may conflict with licensing agreements or may void applicable warranties. Exceptions sometimes may be made for purposes of academic research or employee work with approval from the Chief Information Officer (CIO).

- 11. . College technology users shall not use IT resources to store, display, transmit, or intentionally solicit receipt of material that is or may reasonably be regarded as obscene, sexually explicit, or pornographic except as such access relates to bona-fide, college-related academic or research pursuits or as needed to investigate violations of this policy or laws.
- 12. Users must not misuse or abuse IT resources and privileges. For example, using the College's bandwidth (WIFI and/or wired network) for excessive streaming, intentionally modifying College-maintained hardware and/or software, or excessive printing of documents or web pages that are not solely for classroom and/or business purposes.
- 13. Apart from those devices managed by IT or personal devices reimbursed by the Business Office, personal devices are not allowed to be connected directly to the secure employee network.
- 14. While the College does not routinely monitor individual usage of its computing resources, it does utilize a network firewall to protect the network's integrity and, in certain instances to block certain categories of known malicious or inappropriate content.
- 15. The College reserves the right to investigate suspected violations of this Policy including the gathering of information from users involved and the complaining party, if any, and examination of material on our servers and network. During the College's investigation, the College may suspend user access and/or remove material that violates or potentially violates this Policy. A user authorizes the College to cooperate with (1) law enforcement authorities in the investigation of suspected criminal violations, and (2) system administrators or other network or computing facilities to enforce this Policy. Such cooperation may include providing IP addresses, contact information or other identifying information about a user. IT resources licensed to the College through external contractual agreements may include additional disclosure stipulations.

Consequences of Violations

Users who violate this Policy may be subject to penalties, discipline, monetary penalties, and legal action up to and including suspension, discharge, or revocation of user access.

Effective Date	Motion Number	Document Author	Description of Change
04/18,2023	FF 1009-2024	Information Technology	Clarification of policy language
04/19/2022	FF 1004-2022	Information Technology	Revised to expand and clarify the policy language.
02/28/2017	FF 1007-2017	Information Technology	Initial Release