

HIGHLAND COMMUNITY COLLEGE
GENERAL PERSONNEL POLICY

SUBJECT: Acceptable Computing Policy
BOARD OF TRUSTEE APPROVAL: 01/28/2026

Page 1 of 5
EFFECTIVE DATE: 01/29/2026

Statement

The purpose of this policy is to set forth guidelines so that members of our community may use the campus network and computing facilities in ways that are responsible and respectful of privacy. This policy sets forth the college's expectations of acceptable behavior on the part of computer systems users at Highland Community College (HCC) by providing guidelines for appropriate use of computing and related communication systems and examples of inappropriate use. These standards of acceptable behavior also extend beyond the campus community into the Internet. Just as it is unacceptable to violate others' rights to privacy, property and resources within HCC, it is also unacceptable to violate those rights on systems that are not at HCC but are accessible through HCC's connection to the Internet.

This policy applies to all users of HCC computing systems, including students, faculty and staff, and any others granted the use of college computing resources. It applies to the use of all computing facilities owned, leased, operated or contracted by HCC. As used in this policy, terms such as "computing," "computing/communications systems," "computing resources," etc., refer to all computers, communication systems, and peripherals, software, telephones and systems with similar functions, which are owned by HCC, or which utilize HCC infrastructure such as telephone lines or computer networks.

Although this policy does not attempt to deal specifically with legal issues, college members are responsible to act in compliance with the law, including any federal, state and local laws governing computer and telecommunications use, as well as all other applicable college policies.

Privileges and Responsibilities

Every member of the Highland community who uses computing and related communications systems at HCC, or systems that belong to HCC or which rely on HCC's infrastructure has the responsibilities described in this policy. This includes members of the Highland community who have restricted privileges, such as alumni who may have email access only. Individuals with personally owned computers, but who rely upon the college network to connect those computers (either through an on-campus or remote network connection, such as ethernet or wireless) are expected to abide by the policies set forth in this document. Personally owned computers operating in stand-alone mode or networked through a non-college connection are not covered under this policy, but those users are encouraged to consult the usage policies set forth by their Internet Service Provider.

A fundamental premise of this policy is that anyone sharing computing resources with other individuals should behave as a reasonable, mature and ethical person. The user must recognize that computer systems and networks do not exist in a special environment; on the contrary, use of computers is a form of communication, and every component of a computing environment and every piece of information it contains belong to the HCC, the college community as a whole, or some individual or group within that community.

Access to HCC's computing resources is contingent upon being a member of the college community and adhering to college and Information Technology policies, guidelines and procedures, including this policy. Misuse may result in the loss of access and/or college disciplinary action. For some users and certain systems, access may be authorized by specific departments, research centers or other organizations affiliated with HCC. In such cases, any department- or group-specific policies and guidelines must be adhered to when using resources provided by the department or group. This is in addition to college policies and Information Technology guidelines and procedures.

Any user who suspects a violation of HCC computer use policies, or who has knowledge of potential vulnerabilities or security loopholes in a system or network at HCC, should immediately notify the Highland Community College Information Technology Help Desk.

Maintain the Security and Confidentiality of your Account

Users assume personal responsibility for the use made of their computer accounts. This responsibility begins with selecting a secure password, and involves maintaining the confidentiality of that password and changing the password regularly in order to assure the continued security of your account. For guidance in selecting a secure password. If you believe that someone has made unauthorized use of your account, you should change your password immediately and report the incident to the Highland Community College Information Technology Help Desk.

Respect for Others' Property and Privacy Rights

Users are responsible to respect copyright agreements and intellectual property ownership. Any material that is the work of another, whether explicitly copyrighted or not, should not be distributed by any user without appropriate acknowledgement and/or permission of the creator. Unless permission has been granted by the owner of copyright protected materials, distribution of copyright protected material via the HCC network or computer systems is prohibited. While HCC has been granted permission by software vendors to distribute certain software packages via the network, it is not generally permissible for individual users to distribute that same software to others via the HCC network or computer systems. See the sections in this policy on Misuse and Inappropriate Behavior. While there may be cases in which property rights to particular programs, data, etc., are ambiguous or in dispute, the user must assume that any information not created by himself or herself belongs to someone else and must respect that person's privacy and property rights to that information. (In certain situations, even information created by the user may not belong to that user but rather to HCC or others.) This policy is not intended to limit "fair use" as permitted under the

Copyright Act and users having questions about whether a particular use constitutes a “fair use” may consult Highland Community College Human Resources for guidance.

Improper/Illegal Communications

Any communications that would be improper or illegal on any other medium are equally so on the computer: libelous material, obscene messages, harassment, forgery, threats, etc. However, this is not intended to restrict the free expression of ideas.

Responsible Sharing of Resources

Where a resource such as memory, Central Processing Unit (CPU) time or access to network resources belongs to the whole community collectively, it must be shared.

It is unacceptable to make such excessive use of system or network resources that other users cannot obtain access. Examples include excessive use of CPU time during a period of heavy use on a timesharing system, excessive use of disk space on a system that does not limit such utilization, the use of an excessive amount of network bandwidth in an environment of networked computers, and any activity that makes a system unusable or significantly degrades performance for others. A novice user might be unaware that a particular action constitutes “excessive use” but, without doubt, once a system administrator makes him or her aware of the fact that such an action is unreasonable, that user will be held responsible for any further such infractions. If you are unsure whether your needs constitute excessive use, contact the system administrator. Similarly, if you need an unusual amount of disk space, CPU time or other resources, check with the Director of Information Technology to find out whether this use can be accommodated, rather than risk interfering with the work of others on the system.

Risks of Data Loss and Data Persistence

Although HCC will make efforts to secure the network and college-controlled servers from abuse and damage, it cannot guarantee against data loss by a student, faculty, member or staff, either on a college-operated or an individually-owned computer.

Users should know that even those files that they have “deleted” using the appropriate procedures in the application or operating system, may indeed be recoverable if they exist in a system backup file or other persistent form. If HCC is asked to recover such data by subpoena, it must cooperate, and data that the user believes to have been destroyed may be recovered in the process.

Personal Use

While HCC makes computer resources available primarily to achieve its goals of education and research, and for administrative activities, it realizes the need to encourage the personal use of computing for the convenience of the campus community. Thus, it is reasonable to allow the use of computing resources for computer mail, document preparation, personal or course Web

page publication, or other activity that can facilitate convenience or enhance productivity, to the extent that the activity is within the limits described within the HCC employee handbook. Any personal use of computing resources related to operating a personal business or commercial enterprise is prohibited unless permission to do so has been specifically granted by the Highland Community College President.

We do recognize the difficulty of distinguishing whether certain cases of “personal use” are allowable, such as activities that result in personal financial gain (e.g. checking stock prices online), relate to a commercial business (e.g. college-sponsored technology transfer efforts), or support (but do not constitute operating) a personal business (e.g. a student developing a business plan or a faculty member writing a report for a consulting engagement outside the college). In such cases, we rely on individuals to be responsible and judicious in the use of college’s shared computing resources. In particular ensuring:

- appropriate use of resources (e.g. any such work is completed outside of college time and does not utilize shared resources such as CPU cycles or network bandwidth to a degree that adversely impacts academic or research activities);
- appropriate use of licenses (e.g. do not use software procured with academic use licenses for commercial applications or development, unless the license explicitly permits such use);
- appropriate marketing (e.g. no creation of “.com” domains within Highland Community College’s “edu” domain, no advertising services and products using HCC email accounts, and no advertising using web pages on HCC servers (any server with a ‘.highland.edu’ host name).

In cases of questionable personal use of resources, you may contact helpdesk@highlandcc.edu to determine whether a particular activity is permissible.

We reserve the right to restrict personal use of college systems and networks by an individual or by the community at large, if the use of resources for such activities becomes excessive. If you need unlimited access to computer networks for private or business purposes, you can subscribe to a commercial service.

Privacy

The user must presume that the contents of any other users’ directory are private unless expressly designated otherwise, just as one would presume that the contents of someone’s apartment or office are private. The only exceptions to this rule are: that in some environments, files such as “plan files” may be considered public even if the user has not expressly designated them as such; and that some services such as web pages and anonymous or “guest access” file transfer protocol (ftp) services may be considered to be public, but only for those areas not protected by password and which are “obviously” public. An unprotected account or shared device (such as a shared disk on a networked computer) are not considered to be public unless the name or service expressly indicates that it is. In such cases, any files or other data which would appear to be private in nature, by virtue of the file name or data

stored, even if “publicly accessible” should be considered to be private. The user accessing such files has a responsibility to ask the owner of the files or service if the files are intended to be publicly accessible before the user does more than a “ cursory glance” sufficient to cause the question.

A user can explicitly grant access to his or her directories, files or to services run from his or her systems. However, users who issue general or vague invitations to browse through their files incur a special obligation to protect any material that they do not wish others to see. Indeed, all users are urged to maintain protection levels on their files consistent with the access they are actually willing to give to other users.

Access to Faculty Data

Electronic data on a faculty member’s account, whether stored on a computer in the faculty member’s office or elsewhere under the proprietary control of that faculty member, may not be examined, i.e., the contents of the data read by a person, without the faculty member’s consent, except in cases of emergency or in response to a valid subpoena, search warrant, or order of a court. Posting of data by a faculty member on servers available to the public or to students shall be understood to imply consent, and electronic access given to specific parties by the faculty member will likewise imply consent for those parties to access permitted data. Emergencies may include, for example, but are not limited to, the death, incapacity or disappearance of the faculty member, or the search for and examination of files used for apparently malicious activity in an account which endangers the integrity of shared computers, the network, or other aspects of HCC’s computing infrastructure.

Only specifically designated individuals are permitted to determine what passes for an “emergency.” Such individuals may be specifically designated or may be designated by job position/description. All assignments for individuals or positions will be done by the Director of Information Technology or by a designate of the Director of Information Technology.