5.23 Technology Acceptable Use (Revised 6/25/24)

A. Scope:

1. This policy defines the acceptable use of computing resources owned, operated, and managed by Highland Community College. This policy applies to all persons accessing or using Highland's technology resources, including all employees, students, affiliates, volunteers, or visitors at the College, hereafter referred to as users. This policy is included in the Student Code of Conduct.

B. Policy:

1. In order to promote excellent information and network security posture for Highland Community College, users must comply with institutional and external standards for appropriate use, whether on campus or from remote locations.

2. The purpose of this policy is to outline the acceptable use of computing resources and any information maintained in any form and any medium within the College's computing resources and explain violations of acceptable use. Additionally, all creation, processing, communication, distribution, storage, and disposal of information by any combination of college resources and non-college resources are covered by this policy, which supplements all applicable College policies, including harassment, patent and copyright, student and employee disciplinary policies, and FERPA, as well as applicable federal and state laws.

3. Highland Community College values the privacy rights of all individuals using its computing resources. As a usual business practice, Highland does not routinely monitor individual usage of its computing resources. Nonetheless, users should be aware that all computing resources are the property of Highland. As such, the college may access and monitor computing resources and any information stored on or transmitted through those computing resources, for legitimate business purposes including, but not limited to, system monitoring and maintenance, complying with legal requirements, police investigations, investigating security incidents, and administering this or other Highland policies. Further, to protect systems on the Highland network, the college may, without prior notice if deemed necessary, remove compromised devices from the network, block malicious traffic from entering the network, and prohibit devices within Highland's network from connecting to known malicious outside entities.

C. User Accounts:

1. The use of Highland's computer systems and network requires that the College issue a user account. Every computer user account issued by Highland is the responsibility of the person whose name it is issued. Users are responsible for any activity originating from their accounts that which they can reasonably be expected to control. Under any circumstances, accounts and passwords may not be used by persons other

than those to whom the Highland Network Administrator has assigned them. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident.

2. College recognized clubs and student organizations may be issued a user account. Club advisors shall designate a particular person(s) (e.g., club president) authorized to act on behalf of the club or organization. This person(s) is responsible for all activity on the account and will be subject to College disciplinary procedures for misuse.

3. The college employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that the college cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices using long complex passphrases, employing Multi-Factor Authentication, and guarding their passwords and MFA methods.

D. User Responsibilities:

Users of Highland Community College's technology resources have a shared responsibility with the College's Information Technology Services staff to maintain the integrity of systems, services, and information.

1. User responsibilities include:

   a. To use the College's technology resources responsibly and consistent with the terms of this policy. Users acknowledge college-owned devices and college-contracted services are to be primarily used for college business, and any incidental non-business use will be included in the college's data retention schedule and subject to college FOIA requests.

   b. To access only files and data that the user owns, that are publicly available, or to which the user has been given authorized access by the data owner.

   c. To use only legal versions of copyrighted software in compliance with vendor license agreements.

   d. To comply with College, federal, state, and local regulations regarding access and use of information resources (e.g., College policies regarding the sensitive information and dissemination of information outside the campus, Federal Copyright Act, The Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, Red Flag, HIPAA, codes of professional responsibility, etc.).

   e. To keep technology accounts (computer, network, and application) secure:
      1. Lock Highland devices when leaving unattended.
      2. Access to technology resources is not transferable. Usernames, passwords, or privileges are not to be shared with others, unless specified in Highland's Password Policy.

3. Report suspected unauthorized access to a supervisor or the Information Technology Services department.
4. Allow all ITS Department software and security patches to install.

f. To keep all institutional data in safe-keeping. Specifically, information containing any personally identifiable information (PII) or data of students, staff or others should not leave the institution in a digitally unsecured method and should always be stored on the college's storage drives.

g. To ensure digital content is compliant with other College policies, copyright laws, and applicable local, state, federal laws (including, but not limited to: Americans with Disabilities Act and Web Content Accessibility Guidelines 2.0). Published digital content is not to be used for commercial purposes or for activities not related to the purposes of the College, without written authorization from the College.

h. To inform the ITS department when planning for a new service, or when changing an existing college service or function. The only exceptions are if the service or function do not, in any way, interface with technology.

i. No user shall seek to hold Highland Community College liable for damage resulting from unauthorized interception, use, misuse, damage or destruction of information resources. Each authorized user shall hold Highland Community College harmless and indemnify it for any expense or loss caused by their own unauthorized interception, use, misuse, damage, or destruction of information resources, or by their violation of this policy.

2. Violations of this Policy include, but are not limited to:

a. Illegal Use - Using computing resources to upload, download, transmit, post, or store any material or data that, intentionally or unintentionally, violates any applicable local, state, national or international law, or violates the rules, policies, or procedures of the College or any college department is prohibited. Transmitting, uploading, downloading, or storing any material that infringes upon an existing copyright, trademark, patent, trade secret, or other legal right using computing resources is also prohibited.

b. Threats or Harassment - Using computing resources to transmit material or data that causes or encourages physical or intellectual abuse, damage, or destruction of property, or that knowingly causes or encourages harassment, explicit or implied, is prohibited.

c. Transferring of Use – Permission to use computing resources is granted to individuals and may not be transferred to others. Sharing of a personal username/password assigned to an individual is expressly prohibited. Use of another user's ID or seeking to access another user's account is prohibited.

Similarly, individuals may not use their user credentials to provide access to Highland's wireless network to other individuals. The following will be considered theft of services.

1. Acquiring a username in another person's name.
2. Using a username without the explicit permission of the owner and Information Technology Services.
3. Allowing one's username to be used by another person without the explicit permission of Highland's ITS department.
4. Using former system and access privileges after association with Highland has ended.

d. Malicious Content - Use of Highland computing and messaging systems to transmit any material which contains malicious content, such as malware or phishing scams, or any other content that may damage computer systems or collect or misuse personal information is prohibited.

e. Intercepting Communications - Using packet sniffers, password capture applications, keystroke loggers, and other tools that perform similar behavior or any form of network wiretapping on computing resources is prohibited. Using such tools to diagnose, analyze, or mitigate ongoing service issues or security violations may be permitted when conducted by authorized personnel.

f. Forgery or Impersonation - Falsifying or removing identifying information on computing resources with intent to deceive, defraud, or misguide is prohibited. Impersonation of other persons or groups with the intent to harm is prohibited. Unauthorized use of the College's registered Internet domain name(s) is also prohibited.

g. Unauthorized Access or Penetration Attempts (i.e., "hacking") - Unauthorized access or penetration attempts of Highland computing resources, or a remote entity using Highland computing resources, are prohibited. Users must not use computing resources to impair or damage the operations of any computers, networks, terminals, or peripherals.

h. Service Interruptions - Using computing resources to permit or promote activity that adversely affects the integrity or performance of computing resources is prohibited. Denial of service attacks, forged packet transmission, and similar actions may be permitted when conducted by authorized College personnel.

i. Circumvention of controls – Deliberately circumventing security controls or exploiting vulnerabilities at Highland or any other network from Highland equipment or network is prohibited. Gaining access by exceeding the limits of assigned authorization is likewise prohibited. Users shall not develop or use procedures to alter or avoid the accounting and monitoring of the use of computing facilities. For example, users may not utilize facilities anonymously or

by using an alias. They may not send messages, mail, or print files that do not show the correct username of the user performing the operation.

j. Excessive or Unreasonable Use - Users shall not use information technology resources to excess. Excessive use of information technology resources by a particular user or for a particular activity reduces the amount of resources available to satisfy the needs of other users. Excessive use may degrade or jeopardize system functionality and result in significant costs to the college. Some examples of excess use may include writing a program or script or using an Internet bot to perform a repetitive task such as attempting to register for a class or purchasing event tickets online.

k. Fraudulent Activity - Using computing resources to transmit material or communications to promote a financial scam or wrongdoing is prohibited.

l. Creation, interference with, or transmission of Wireless Signals – Creation of new wireless network requires explicit permission of Highland's ITS department. Interfering with Highland's wireless networks or attaching a device to transmit a Highland network is strictly prohibited.

m. Personal Gain - Computing resources are not to be used for commercial purposes or personal financial or other gains.

n. Abuse of communication systems - Sending unsolicited messages, which in the College's judgment, is disruptive to system resources or generates a significant number of user complaints is prohibited. This includes using any college communication system (email, text, app, or phone calls) to send spam, bulk, or malicious messages, including commercial advertising, political tracts, or other inappropriate use of system distribution lists. Bulk messaging should not be the venue for any all-campus conversations.

o. Institutional Image - Unless resources are used to meet the College's purpose, to support our educational and community values, and/or to support our programs and initiatives, users are prohibited from accessing, submitting, publishing, displaying, or posting any defamatory, inaccurate, abusive, obscene, profane, sexually oriented or explicit, threatening, racially offensive, harassing, or illegal material.

p. Abuse of incidental personal use - Incidental personal use must not:

    1. Be illegal.
    2. Interfere with a Highland employee's job responsibilities/work.
    3. Interfere with the legitimate education and business purposes of Highland.
    4. Result in any measurable cost to the College.
    5. Adversely affect the availability, integrity, or reliability of Highland IT systems or cause harm to the activities of others using the IT systems.

6. Violate this policy or other College policies.
7. Be inconsistent with the College's status as a state entity and its non-profit, tax-exempt status.

q. Physical Security - Unauthorized access to, destruction, extension, or alteration of, theft, damage, or tampering of any physical computing resources, including computer workstations, kiosks, card swipes, printers, audio-visual equipment, telephone/fax equipment, classroom equipment, or wiring closets is prohibited. This applies to all network wiring, hardware, and in-room jacks. Users shall not use the network to provide Internet access to anyone outside of the College community for any purpose other than those that are in direct support of the academic mission of the College.

E. Reporting & Enforcement:

1. Violations of this Policy may be reported through one's supervisor, the Highland ITS Service Desk, or as otherwise permitted through College policy.

2. The College may, without notice, disable or suspend access to the system as part of any routine maintenance or concern over the safety and security of the system.

3. Users who violate this policy may be denied access to college computing resources and may be subject to other penalties, including financial costs, and/or disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the college disciplinary procedures applicable to the user. The college may suspend, block, or restrict access to an account, independent of such procedures, when it reasonably appears necessary to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability. The college may also refer suspected violations of applicable law to appropriate law enforcement agencies.

4. When Highland ITS becomes aware of a possible violation, an investigation will be initiated with relevant campus offices, such as the appropriate Vice President, Human Resources, and local authorities. Users are expected to cooperate fully in such investigations when requested.

5. To prevent further unauthorized activity during such an investigation, Highland ITS may suspend authorization for the use of all computing facilities for the user(s) involved in the violation.