Highland Community College

Information Technology Services
Acceptable Use Guidelines
Updated 2015

Highland Community College provides technology resources to meet the College's purpose, to support our educational and community values, and to support our programs and initiatives. Highland Community College's Information Technology Services organization's goal is to provide high quality services to the campus community. To ensure that our high standards are met, we have certain expectations regarding the use of technology resources at the College.

Access to Highland Community College technology resources--computing facilities, network services, servers, equipment, software, applications, information resources, printing and scanning services, and user and technical support provided by Information Technology Services staff--is a privilege, not a right. This privilege is extended to all users-- faculty, staff, students, trustees, alumni/ae, affiliated individuals and organizations, partner non-profits and Pre-K-12 schools. Accepting access to this technology carries an associated expectation of responsible and acceptable use.

This "Acceptable Use Guidelines" document describes activities that Highland Community College considers acceptable use, as well as violations of use, of technology resources. The examples listed are not exhaustive and may change from time to time as technology and applications change. The examples are provided solely for guidance to users. If you are unsure whether any use or action is permitted, please contact the Director, Information Technology Services for assistance at 815-599-3599.

While there are cases in which the use of technology resources is deemed not responsible or not acceptable, there are also more serious cases in which technology resources are used in the conduct of behaviors which violate College policies, code of conduct, or local, state, or federal law. Though the use of technology resources is the focus of this document, members of the Highland Community College community and others using Highland Community College’s technology resources are advised that use may also be governed by other College policies including but not limited to those in the student handbook, College catalog, and other policies governing academic, student life, or personnel matters at the College or agreements between the College and affiliated organizations. Highland Community College's technology and information resources are not to be used for commercial purposes or non-College related activities without written authorization from the officer(s) of the College that have been so designated (contact the Director, Information Technology Services for further information).
Highland Community College reserves the right to enforce applicable penalties in accordance with College policies, code of conduct, or local, state, or federal law and/or immediately terminate access to College systems and network services to any user in cases where technology resources have been used in a manner that is disruptive or is otherwise believed to be in violation of "acceptable use" or other College policies or law. The College will act in accordance with the provisions of the Digital Millennium Copyright Act in the event of notification of alleged copyright infringement by any user.

The College retains control, custody and supervision of all College provided computer technology. To ensure proper network performance and security, as well as appropriate use, authorized Information Technology Services staff may monitor and record user activity. No user shall have expectations of privacy in their use of computer technology, including e-mail messages and stored files.

Although Highland Community College takes measures to safeguard integrity and confidentiality, it in no way guarantees the safety or security of information resources. Highland Community College disclaims liability for the unauthorized interception, use, misuse, damage or destruction of information resources. No student, faculty member, staff member, or authorized 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 his/her own unauthorized interception, use, misuse, damage, or destruction of information resources, or by his/her violation of this Acceptable Use Guideline document.

Thousands of current and future students, faculty, staff, alumni, and donors are utilizing social media sites such as Facebook, Twitter, LinkedIn, YouTube, MySpace, and a whole host of blogging sites and comment interfaces to stay personally and professionally connected. HCC believes that having a presence in these areas will allow the College to broadcast information and interact with the public in ways that will further Highland's mission, vision, and core values.

Social media sites are powerful communication tools that have a significant impact on organizational and professional reputations. Because they blur the lines between personal voice and institutional voice, Highland Community College has developed guidelines, located within this document, to help clarify how best to enhance and protect personal, professional, and institutional reputations when participating in social media.

Both in professional and institutional roles, employees need to follow the same behavioral standards while participating in social media as they would in real life situations. The same College policies, code of conduct, professional expectations, and guidelines for interacting with students, parents, alumni, donors, media, and other constituents apply online as in real world situations. Employees are personally accountable for anything they post to any social media sites.

User and Staff Responsibilities:

As a user or staff member of Highland Community College's technology resources, you have a shared responsibility with the College's Information Technology Services staff to maintain the integrity of our systems, services, and information so that high quality services can be provided to everyone. Your responsibilities include:

1. To use the College's technology resources responsibly and appropriately, respecting the rights of other users to system, services, and information access 24 hours per day, 7 days per week.

2. To respect all contractual and license agreements, privacy of information, and the intellectual property of others.

3. 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.).

4. To exercise due diligence in protecting any personally owned computer you connect to the Highland Community College wireless network from viruses, worms, and security vulnerabilities by regularly using anti-virus software.

5. To keep your technology accounts (computer, network, application) secure. If you suspect unauthorized access, report it to your supervisor or the Information Technology Services department.

6. To not share your privileges with others. Your access to technology resources is not transferable to another member of the Highland Community College community, to family members, or to an outside individual or organization.

7. To comply with posted policies governing use of public computing facilities.

8. To present a web page that reflects the highest standards of quality and responsibility. As web page owner, you are responsible to ensure that both the content of your web page and all links and references from your web page are consistent with this and other College policies, copyright laws, and applicable local, state, federal laws. Published web pages are not to be used for commercial purposes or for activities not related to the purposes of the College, without written authorization from the College.

9. To understand the implications of sharing personal information or data via the Internet, e-mail, Instant Messaging or other services that either are open to access by others on and off-campus, or that can be forwarded to others.

10. To keep all institutional data in safe-keeping. Information containing any personal data of students, staff or others should not leave the institution unsecured.

11. To ensure all information is stored to the network (H: and G:) and not to local computer hard drives (C:).

Examples of Violations of "Acceptable Use"

Unauthorized Access Unauthorized Accounts

1. Attempting to obtain unauthorized access or circumventing user authentication or security of any host, network or account ("cracking"). This includes accessing data

not intended for the user, logging into a server or account the user is not expressly authorized to access, or probing the security of systems or networks.

2. Supplying or attempting to supply false or misleading information or identification in order to access Highland Community College's technology resources.

3. Sharing your passwords or authorization codes with others (computing, e-mail, applications, etc.)

4. Using technology resources for unauthorized or illegal uses.

5. Logging onto another user's account; sending e-mail, etc. from another user's account or device or from an anonymous account.

6. Unauthorized use of the College's registered Internet domain name(s).

7. Changing your Highland Community College-issued machine name to a name that is different from that assigned by Information Technology Services.

Unauthorized Access to or Use of Services and Equipment

8. Attempting to interfere with service to any user, host, or network. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service, port scans and attempts to "crash" a host.

9. Use of any kind of program/script/command designed to interfere with a user's computer or network session.

10. Intentionally damaging or tampering with a computer or part of a computer system.

11. Knowingly spreading computer viruses.

12. Modifying the software or hardware configuration of College technology resources, including dismantling computers in the lab for the purposes of connecting a notebook computer to the peripherals.

13. Excessive use of technology resources for "frivolous" purposes, such as game playing, streaming non-educational audio/video, or downloading files. This causes congestion of the network or may otherwise interfere with the work of others, especially those wanting to use public access PCs or network and Internet resources.

14. "Hacking" on computing and networking systems of the College or using the College's network to “hack” other networks.

15. Setting up wireless access points (WAPs).

16. Employees are not to use technology services excessively for personal use while performing their regular assigned duties.

17. 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.

Unauthorized Use of Software, Data & Information

18. Inspecting, modifying, distributing, or copying software or data without proper authorization, or attempting to do so.

19. Violating software licensing provisions.

20. Installing software on College machines without appropriate authorization (from Information Technology Services).

21. Installing any diagnostic, analyzer, "sniffer," keystroke/data capture software or devices on College technology resources.

22. Breaching confidentiality agreements for software and applications; breaching confidentiality provisions for institutional or individual information.

Unauthorized Use of Email/Internet Messaging

23. Harassment or annoyance of others, whether through language, frequency or size of messages.

24. Sending unsolicited bulk mail messages ("junk mail" or "spam") which, in the College's judgment, is disruptive to system resources or generates a significant number of user complaints. This includes bulk mailing of commercial advertising, political tracts, or other inappropriate use of system e-mail distribution lists. Bulk mail should not be the venue for any all-campus conversations.

25. Forwarding or otherwise propagating chain e-mail and pyramid schemes, whether or not the recipients wish to receive such mailings. This includes chain e-mail for charitable or socially responsible causes.

26. Malicious e-mail, such as "mailbombing" or flooding a user or site with very large or numerous items of e-mail.

27. Forging of e-mail header envelope information.

28. Forging e-mail from another's account.

Unauthorized Use of Web Pages & Servers

29. Posting content on your web page that provides information on and encourages illegal activity, or is harassing and defaming to others.

30. Linking your web page to sites whose content violates College policies, local, state, and/or federal laws and regulations.

31. Running web sites that support commercial activities or running server systems under the College's registered domain name, HIGHLAND.EDU or variation thereof, without the College's authorization.

Social Media Guidelines and Acceptable Uses
General Posting Recommendations

1. Be honest about your identity. If you desire to post about Highland in an unofficial capacity, please identify yourself as a Highland faculty or staff member. Never conceal your identity for the purpose of promoting Highland through social media. An excellent resource about transparency in social media sites is the Blog Council’s “Disclosure Best Practices Toolkit” at http://blogcouncil.org/disclosure/

2. Be accurate in your posts**.** Make sure that you have all the facts before you post. It’s better to verify information with a source first than to have to post a correction or retraction later. Cite and link to your sources whenever possible. If you make an error, correct it quickly and visibly. This will earn you respect in the online community.

3. Be respectful to others. You are more likely to accomplish what you want if you are positive and respectful while discussing a bad experience or disagreeing with an idea or person.

4. Be a valued member of the sites in which you are participating. If you join a social network like a Facebook group or comment on a blog, make sure you are contributing valuable input. Refrain from posting information about topics like Highland events unless you are sure it will be of interest to readers. Self-promoting behavior is viewed negatively and can lead to you being banned from certain sites or groups.

5. Take care to think before you post. There’s no such thing as a “private” social media site. Search engines can turn up posts long after the publication date. Comments can be forwarded or copied. Archival systems save information even if you delete a post. If you feel annoyed or passionate about a subject, it’s advisable to hold off posting until you are calm and clear-headed.

6. Maintain confidentiality at all times. Do not disclose confidential or proprietary information about Highland, its students, its alumni or your fellow employees. Use good ethical judgment and follow College policies and federal requirements, such as

FERPA and HIPPA. As a guideline, don’t post anything that you would not present at a conference.

7. Respect College time and property. As stated in Section 5.23 of the College Policy Manual, computers and your work time are to be used for College-related business. It is appropriate to post at work if your comments are directly related to accomplishing college-related goals, such as seeking sources for information. You should maintain your personal sites on your own time using non-Highland computers.

Official Highland Community College Social Media Accounts

To ensure that any and all interactions on behalf of Highland represent the College’s best interests, the following guidelines have been crafted for those Highland employees authorized to participate and/or maintain official social media sites on behalf of the College. These guidelines are designed to be broad in nature to accommodate differences in online venues while maintaining a universal code of conduct.

8. To be recognized by the College as an official HCC social media account, the account administrator(s) must seek approval from the Community Relations (CR) office. The CR office will review all social media inquiries. This office should also be used as a resource for the college community for any social media needs. The CR Office will ensure the pages are set up properly according to the social media site’s policy.

9. All social media accounts officially recognized by the College must have a HCC faculty or staff member as an administrator at all times. In the event that accounts allow for multiple administrators, the CR office may request administrator privileges.

10. Should an HCC employee account administrator leave the College for any reason or no longer wish to be an account administrator, it is that individual's responsibility to designate another HCC employee to be an account administrator prior to removing himself or herself from that role. The CR office should be notified when a new administrator takes over. College employees identified as account administrators are held responsible for managing and monitoring content of their officially recognized accounts.

11. Administrators are responsible to remove content that may violate the College’s policies. If you have questions regarding the appropriateness of a post to a site that you administer, please contact the CR office.

Content

12. Use good judgment about content and respect privacy laws. Do not include confidential information about the College, its staff, or its students.

13. You may post any content that is not threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise injurious or illegal.

14. Refrain from posting personal opinions on official College social media accounts. Refrain from using the HCC name to promote any personal opinion, product, cause, or political candidate.

15. By posting content to any social media site, you agree that you own or otherwise control all of the rights to that content, that your use of the content is protected fair use, that you will not knowingly provide misleading or false information, and that you hold the College harmless for any claims resulting from the content.

16. HCC has the right to remove any content for any reason, including but not limited to, content that it deems threatening, obscene, a violation of intellectual property rights or privacy laws, or otherwise injurious or illegal.

17. When using or posting online material that includes direct or paraphrased quotes, thoughts, ideas, photos, or videos, always include citations. Provide a link to the original material if applicable.

18. Refrain from using information and conducting activities that may violate local, state, or federal laws, and regulations.

Payment Card Industry (PCI) Compliance Guidelines

1. PCI Self-Assessment Questionnaire number 3.3: The PAN (Personal Account Number) is masked when displayed and the last for digits are the maximum number of digits to be displayed.

2. PCI Self-Assessment Questionnaire number 4.2: All PAN's (Personal Account Numbers [credit card numbers]) are not to be sent via end-user messaging technologies, such as testing, instant messengers, email, etc.

3. PCI Self-Assessment Questionnaire number 9.9 (a): The College must maintain a list of devices that are capable of capturing payment card data via direct physical interaction with the card.

4. PCI Self-Assessment Questionnaire number 9.9 (b): College employees authorized to operate equipment related to capturing payment card data via direct physical interaction with the card must perform realtime inspections of the equipment to look for any tampering (such as card skimmers) or substitution. Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. Report any suspicious tampering or substitution to the Vice President, Administrative Services immediately.

5. PCI Self-Assessment Questionnaire number 9.9 (c): The College must train employees during PCI security training to look for suspicious behavior, device

tampering, and substitution. No College employee may purchase any device or service relating to the processing of credit card information without approval from the Vice President, Administrative Services.

6. PCI Self-Assessment Questionnaire number 12.3.1: Explicit approval by authorized parties to use the technologies: Staff who are responsible for handling credit card transactions as a part of their job duties need to be authorized in writing (or email) to operate a credit card swipe terminal or to have an account set up for use in an online payment system.

7. PCI Self-Assessment Questionnaire number 12.3.2: Authentication to systems is required by staff to access critical technologies

8. PCI Self-Assessment Questionnaire number 12.3.3: The College maintains a list of all such devices and personnel with access, considered to need access to critical technologies.

9. PCI Self-Assessment Questionnaire number 12.3.5: Acceptable locations for use of the technologies: Highland Community College currently approves acceptable locations for use of the credit card swipe terminals to be limited to the Cashier's Office and the Bookstore. Use of TouchNet and associated applications for online credit card processing shall be used in the cashier's office, accounting staff offices, IT offices, and the bookstore. Use of SeatAdvisor is limited to the Box Offices.

10. PCI Self-Assessment Questionnaire number 12.3.6: Acceptable locations for use of the technologies: Highland Community College currently approves acceptable locations for use of the credit card swipe terminals to be limited to the Cashier's Office and the Bookstore. Use of TouchNet and associated applications for online credit card processing shall be used in the cashier's office, accounting staff offices, IT offices, and the bookstore. Use of SeatAdvisor is limited to the Box Offices. The network locations of these technologies are maintained.

11. PCI Self-Assessment Questionnaire number 12.3.8: The College maintains an automatic disconnect timeout for remote access technologies after a period of inactivity lasting 15 minutes.

12. PCI Self-Assessment Questionnaire number 12.3.9: Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.

13. PCI Self-Assessment Questionnaire number 12.5.3: The Vice President of Administrative Services is responsible for establishing, documenting, and distributing security incidents, response, and escalation procedures to ensure timely and effective handling of all situations.

14. PCI Self-Assessment Questionnaire number 12.8.3: The College performs due diligence in evaluating the reputation of a vendor to ensure they have a good and clean record and reputation with PCI security.

15. PCI Self-Assessment Questionnaire number 12.8.4: The College performs an annual inspection on all service providers to validate their PCI compliance using the PCI council's lookup tool. These checks are performed at least annually.