Proposed Black Hawk College
RESPONSIBLE USE GUIDELINES AND PROCEDURES

I. Purpose:

College guidelines for acceptable use of information technology resources made available to students, faculty and staff, and any non-College individuals and entities specifically authorized to use these resources. (User)

The same acceptable standards for all users with regard to the use of facilities, equipment and tools, as well as acceptable standards of behavior toward individuals while using these resources, apply to the use of information technology resources as well. The ability to use these resources is a privilege, not a right or guarantee, based on College priorities and available funding. No one can or should assume that because this policy is silent on a particular act or behavior, or that just because one is capable of doing something, that it is then acceptable, condoned, or legal.

II. Reference to Existing Policies/Procedures/Laws:

The Board of Trustees, through policies, guidelines and regulations has already established acceptable uses of College resources. The Board has also defined and established processes available to all students, faculty and staff regarding such issues as harassment, standards of behavior, plagiarism, conflict of interest and unethical conduct, as evidenced in the Board of Trustees' policies and the Black Hawk College Student Handbook. There already exist federal, state, and local laws, rules and regulations regarding theft, copyright infringements and other unlawful acts. Those same disciplinary actions that apply to the misuse of other resources and behaviors may be applied to misuse of information technology resources. All users who request and/or are given access to College-owned and operated information technology resources agree to use those resources in a manner consistent with the mission of the College and in compliance with Board of Trustees' policies, as well as all applicable laws, procedures, rules and regulations.

III. Definitions

A. **College network –** All technology equipment, software resources and any related technology resources that are administered, allocated and managed by and for the College, are considered to belong to the College network, whether in a networked environment or stand alone, including equipment owned by the College used in an off-site location.

B. **System Administrator/s –** The person/s responsible for administering and managing resources of the College network. System administrators shall perform their duties fairly, in cooperation with the user community, College policies and funding resources. System administrators for both educational software and functional applications shall respect the privacy of users, in as far as reasonably possible.

C. **WWW/electronic publishing/portal communications –** Any site created and maintained on the World Wide Web, whether personal or an official instrument of the College. Portal is known as "myBlackhawk."

D. **E-mail –** Electronic communications, or e-mail, is available for communications in a responsible manner, in accord with College policy. It is intended for communication between individuals and clearly identified groups of interested individuals, not for mass broadcasting.

E. **Password –** Passwords are unique alpha/numeric combinations provided only for the user's personal use, not to be shared with anyone. Doing so may permit access to services not authorized to another user.

F. **Computer Hardware –** Computer hardware consists of computer workstations and their peripherals (monitors, keyboards, mice, printers, scanners, etc.) and the network equipment to which these hardware are connected.

G. **Computer Software –** Computer software consists of computer language/programming instruction that enables computer hardware to operate and perform functional tasks, and may be stored on various media.

H. **Telephone/Communications Resources –** Telephone/communications resources are hardware and software which enable voice and data transmission over telephone/data lines.

III. User Responsibilities

Users are expected to comply with those legal requirements and standards regarding appropriate behavior related to the use of computer and telephone systems, as well as any requirements that may be approved by the Board of Trustees from time to time.

A. The User is expected to abide by College security requirements and will:

1. use the College's computer or network resources only with proper authorization.
2. neither endanger the security of any College computer or network facility nor willfully interfere with others' authorized computer use.
3. connect to College networks only with equipment/computers meeting College technical and security standards.
4. provide reasonable security to one's passwords and respect the privacy and security of others' passwords. If it is suspected that a password has been discovered it should be changed immediately. Users are also

prohibited from attempts to alter their identity, either through the use of another's password, or to establish a false identity.

5. recognize that confidential information must be protected appropriately, as the College cannot guarantee the privacy of computer files, electronic mail, or other information stored on or transmitted by computer unless special arrangements are made.

B. The User is expected to abide by existing legal requirements and those that may be added from time to time and will:

1. abide by law in not participating in computer theft, computer trespass, invasion of privacy, identity theft, computer forgery, password disclosure, misleading transmittal of names or trademarks.
2. abide by the laws of copyright and/or license agreements.
3. understand that the College will not defend the user against any charges of criminal acts outside of the scope of employment involving the use of College-owned resources.
4. use the College's resources only for College business or coursework and not to conduct any non-College business. Occasional, limited, appropriate personal use of the College IT resource is permitted if that use does NOT: (1) interfere with the user's work performance; (2) interfere with any other user's work performance; (3) interfere with the ability of other students to accomplish their coursework; (4) have undue impact on the operation of the College IT resources; (5) violate any other provisions of policy or practice standards of the College.
5. take responsibility for the materials they transmit through College e-mail or portal resources and not violate College policy.
6. recognize that they may not harass, threaten, or otherwise cause harm to specific individuals through electronic communications.
7. not create what even a casual observer might reasonably perceive to be an atmosphere of harassment, including sexual harassment, even if that person just happens to be passing by. The casual observer may be anyone such as a fellow student, faculty or staff member or employee.

C. Users shall adhere to a standard of behavior that is not disruptive to the business of the College and will:

1. not impede, interfere with, impair or otherwise cause harm to the activities of others;

2. take care not to download or post to College computers, or transport across College networks, material that is illegal, proprietary, subject to copyright protection, in violation of College contracts, or that otherwise is damaging to the institution.

a. use the College's communication facilities neither to attempt unauthorized use, nor interfere with others' legitimate use of any computer or network facility anywhere.

b. share computing resources in accordance with policies set for computers involved.

c. use caution in downloading or distributing information and shall not create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any College computer or network resource, regardless of whether any demonstrable harm results.

d. use available software and hardware "as is" without attempting to modify or reconfigure the software or hardware of any College computer or network.

e. be cautious of receiving fake electronic mail, hoaxes, scams, and false warnings, and not open or redistribute any suspicious items.

f. use caution when sending out any message that might appear to be an official communication from the College.

D. Users will be good stewards in the care and safeguarding of files and records and will:

1. take care to back-up files periodically and regularly, to prevent loss of data.

2. recognize that these responsibilities extend beyond the confines of any employment or contractual relationship with the College, and that any attempt to destroy or alter College records for purposes other than routine maintenance, whether hard copy or electronic, will be subject to disciplinary/legal action.

3. comply with periodic requests to alter/change passwords and any training requirements associated with continued use and access to the College's resources.

4. be certain to not leave themselves logged into any unattended system.

III. College Responsibilities

A. The College is expected to adhere to industry standards and other best practices with regard to computer and telephone systems to provide adequate access to these resources with the optimum service levels possible, in accordance with legal requirements and Board of Trustees' policy, within the approved budget. The Vice President for Information Technology Systems is charged with directing and managing these efforts.

B. The College makes no warranties of any kind, either express or implied, that the functions or services provided by or through technology resources will be error free or without defect. The College will not be liable for any damage users may suffer, including but not limited to loss of data, service interruptions or failure to deliver services. In addition, the College makes no representation or warranties, either express or implied, for data, information and materials obtained over the Internet and will not be liable for any damage users may suffer as a result of relying upon such data or information.

C. College system administrators are expected to abide by College standard security requirements and will:

   1. maintain the maximum access to computing resources possible, with consideration to environmental conditions, security and safety issues, and budgetary resources.
   2. take all reasonable precautions to protect College systems.
   3. take reasonable steps to assure that confidential information is protected appropriately, recognizing that the College cannot guarantee the privacy of computer files, electronic mail, or other information stored on or transmitted by computer.

D. College system administrators will be good stewards in the care and safeguarding of files and records and will:

   1. provide access to computers and networks to the extent permitted by law, budgetary resources, technical capability, and adherence to established standards approved by the Vice President for Information Technology Systems.
   2. complete system server back-ups as often as is necessary to safeguard files and records.

E. College system administrators shall adhere to a standard of behavior that is not disruptive to the business of the College and will:

   1. reserve the right to block incoming mass mailings ("spam"), and to block all Internet communications from sites that are involved in extensive spamming or other disruptive practices.
   2. respect privacy and refrain from snooping.
   3. permit officially recognized College organizations to send appropriate announcements to all their members by e-mail and to facilitate the College's need to send bulk e-mail, including disseminating administrative

notices, notifying students of educational opportunities, or otherwise carrying on the work of the College subject to reasonable approval or authorized procedures.

4. treat all users fairly and equitably and not interfere with users' electronic communication, especially in any way that would be interpreted as favoring one side of a controversy or suppressing an unpopular opinion or topic.

F. College system administrators are expected to abide by existing legal requirements and those that may be added from time to time and will:

1. provide computers and networks to serve the College community in the furtherance of the College's mission, in accordance with College policies and procedures, federal, State of Illinois and local laws and regulations.
2. understand that a system administrator is not the judge, jury and enforcer in cases of computer misuse, and refer all cases of suspected misuse to the Public Safety office.

G. College system administrators will take all reasonable measures to insure adequate safety of College computer resources and the data maintained thereon and will:

1. provide opportunities for training to College users, and otherwise make every reasonable effort to inform users of Board of Trustees' policies with regard to the use of computing resources.
2. develop and publish a schedule for users of required password changes, implementing such with as little interruption of service as is possible.
3. apprise users of planned interruptions of service for maintenance and back-ups, when required, at least 72 hours in advance.
4. apprise users of unplanned, but necessary and required interruptions of service as soon as is practically possible.
5. restore service to users as quickly as is practically possible.

H. College system administrators are required to establish reasonable and fair standards for access by users to College computer resources. It is considered an abuse of College policy to try to gain access to systems, files, or communications for which the user does not have authorized access, whether through security holes or other loopholes. Legitimate use of a computer network does not extend to whatever an individual is capable of doing. Users are asked to report suspected violations of security to the Vice President for Information Technology Systems or his/her designee, who will investigate the matter through established procedures.

IV. Privacy Issues of Computer Use and Communications

Users are reminded that all information created or received for work purposes and/or contained in College computing equipment files, servers or e-mail are depositories and are public records, and are available to the public unless an exception to the Illinois Public Information Act applies. Thus, users should have no expectation of privacy. The College respects the desire for privacy and voluntarily chooses to refrain from routinely inspecting user files and electronic/telephonic communications. However, the College may monitor access to the equipment and networking structures and systems for such purposes as insuring the security and operating performance of its systems and networks; reviewing employee performance; and enforcing College policies, procedures, guidelines, and applicable laws.

Examination of users' files, email, or network transmission contents by the Information Technology staff or its contractors must be authorized beforehand by written approval from two members of President’s Cabinet.

V. World Wide Web/Electronic Publishing

The development and maintenance of a personal website or homepage is permitted as a learning tool, through the College’s computing resources. Electronic publishers are expected to observe all applicable laws, rules and regulations, are solely responsible for content and maintenance of personal sites, and will not in any way indicate or imply that such material is endorsed by the College. Personal homepages/sites shall contain a disclaimer stating “that the page/site is not endorsed, sponsored or provided by or on behalf of Black Hawk College.”

VI. Computer Hardware and Software

A. Warranty Agreements

It is the practice of the College to respect all manufacturer warranty agreements and to service College-owned computer hardware within manufacturer guidelines by authorized warranty service technicians. College authorized users may not attempt to repair or modify hardware that is under warranty agreement and that is part of the College hardware inventory, without the express written permission of the manufacturer.
It is also the practice of the College to respect all computer software copyrights and to adhere to the terms of all software licenses to which Black Hawk College is a party. Black Hawk College will take all steps necessary to prohibit users from duplicating licensed software or related documentation for use either on College premises or elsewhere unless the College is expressly authorized to do so by agreement with the licensor.

VII. Policy Assurance

A. Any suspected criminal activities will be referred to the Public Safety office and handled according to policies established therein.

B. Any suspected activities of harassment related to use of information technology resources will be referred to the Equal Employment Office/ Affirmative Action.

C. Any suspected security breaches will be referred to the Vice President for Information Technology Systems or his/her designee and handled according to established policies.