DEFINITION

Technological and information resources are defined to include electronic data and records; software; networking tools; remote access devices; electronically recorded voice, video, and multimedia communications; and other electronic devices used primarily for the transmission, storage, or utilization of electronically communicated information.

USE OF COLLEGE DISTRICT TECHNOLOGICAL AND INFORMATION RESOURCES

College District technological and information resources are provided to allow faculty, staff, and students to pursue the central educational mission of the College District and are to be used to the extent that they promote that mission either directly in teaching and research or indirectly in supporting the offices that maintain College District operations. Incidental personal use that does not otherwise violate this policy or have an adverse effect on College District resources shall be permitted. Technological and information resources shall be accessed and used in an ethical manner consistent with the institution's Core Values, which include a passion for learning, service and involvement, creativity and innovation, academic excellence, dignity and respect, and integrity. All users of technological and information resources are to adhere to legal and professional standards, to support the mission, and to act in the best interests of the College District.

All users of technological and information resources are responsible for the protection of College District assets to which they are assigned and for not compromising the accuracy, integrity, and confidentiality of the information to which they have access. Resources are not to be abused or employed in such a way as to interfere with, or cause harm or damage to, another person, institution, or company within or outside the College District. While the College District encourages the exploration of educational and scholarly interests through the use of its technological resources, respect for the rights and privacy of others shall be observed. Those who are authorized to access confidential files shall respect the privacy rights of others and use data only for legitimate academic or administrative purposes.

All users of College District technology resources shall comply with the following policies, procedures, and security controls.

ACCESS

Many of the technological and information resources of the College District may be accessed by all employees and students of the College District and by the public as well. However, access to some resources is restricted. The appropriate administrators shall determine and authorize the appropriate degree of access.

Users shall implement best practices in taking precautions to prevent the unauthorized use of their access codes. In choosing access codes, users shall avoid the use of common words, proper

names, readily associated nicknames or initials, and any other letter or number sequences that might easily be guessed. Users shall be held accountable for their own actions performed under their access codes and shall be subject to appropriate disciplinary action if violations occur from the actions of other individuals as a result of user negligence in protecting the codes. Users are responsible for changing access codes on a regular basis. If an access code becomes compromised, users shall change it immediately upon becoming aware that said code has been compromised.

Users shall not attempt to access, search, or copy technological and information resources without the proper authorization. No one shall use another individual's account without permission, and active sessions shall not be left unattended. Providing or using false or misleading information in order to gain access to technological and information resources shall be prohibited. Users shall not test or attempt to compromise internal controls, even for purposes of systems improvement. Such actions require the advance, written approval of the authorized administrator or must be included among the security evaluation responsibilities of one's position. Violations shall be reported to the chief information systems officer in the office of information technology.

PROTECTING CONFIDENTIALITY

Unless disclosure is a normal requirement of a user's position and has been so authorized, no user shall disclose:

1. Confidential information that is protected by the Family Educational Rights and Privacy Act (FERPA);
2. Personnel records; or
3. Other materials commonly recognized or considered as sensitive or confidential.

All users with access to confidential data shall safeguard the accuracy, integrity, and confidentiality of that data by taking precautions and performing office procedures necessary to ensure that no unauthorized disclosure of confidential data occurs. Such precautions and procedures include, but are not limited to, securing storage of data backups, protecting sensitive data with access codes, and only storing sensitive materials on the College District's network, including College District-approved or College District-contracted external sites such as publisher websites for a course being offered by the College District.

Information regarding the confidentiality of student educational records may be found in the student handbook or by contacting the registrar.

PRIVACY

For purposes of this policy, privacy is defined as the right of an individual or an organization to create, maintain, send, and receive electronic data, software, and communications files that are safe from examination and disclosure by unauthorized parties. The College District recognizes that individuals have a substantial interest in and reasonable expectation of privacy. Accordingly, the College District respects the privacy rights of all users of the College District's technology resources.

The College District shall not monitor users' private electronic data, software, and communications files as a routine matter. Users should note that some electronic files are copied to backups and stored for indefinite periods in centralized locations. In such instances, user deletion of an electronic file, such as an e-mail message, may not delete a previously archived copy of that file.

It is a violation of College District policy for any member of the College District community to access College District databases to engage in electronic "snooping," or to use College District technological resources for the purpose of satisfying idle curiosity about the affairs of others, with no substantial business purpose for obtaining access to such files.

The College District reserves the right to access and to disclose the contents of an individual's electronic data, software, and communications files; however, the College District will do so after obtaining the proper approvals only when a legitimate need exists and the urgency of the need is sufficiently strong to offset the College District's commitment to honor the individual's privacy. Such grounds include, but are not limited to:

1. Maintaining system integrity, for example, tracking viruses;
2. Protecting system security;
3. Investigating indications of impropriety;
4. Protecting the College District's property rights; and
5. Meeting legal obligations, for example, subpoenas and open records requests.

COPYRIGHT ISSUES

Copyright is a form of protection the law provides to the authors of "original works of authorship" for their intellectual works that are "fixed in any tangible medium of expression," both published and unpublished (Title 17, United States Code). It is illegal to violate any of the rights provided by the law to the owner of a copyright. The College District respects the ownership of intellectual material governed by copyright laws. All users of the College District technology resources shall not knowingly fail to comply with the copy-

right laws and the provisions of the licensing agreements that apply to software; printed and electronic materials, including documentation, graphics, photographs, multimedia, including musical works, video productions, sound recordings, and dramatic works; and all other technological resources licensed or purchased by the College District or accessible over network resources provided by the College District. The user shall be responsible for reviewing individual author, publisher, patent holder, and manufacturer agreements for software, programs, and applications loaded by the user onto College District hardware, equipment, and web resources.

In compliance with the requirements of the Digital Millennium Copyright Act of 1998 (DMCA), any user of the College District's technology resources who violates the digital copyright laws for the first time shall be reminded of the laws, and the software or licensing violations shall be removed. A second violation shall result in removing the software or licensing violations, retraining of the user in copyright procedures, and taking appropriate disciplinary action. A third violation shall require the College District to remove the user's network and Internet access and take further disciplinary action, which may include termination from College District employment or student status. In addition, any violation of digital copyright laws by a student or by a College District employee that results in demonstrable harm to the College District's network or disruption of classroom activities shall be addressed as a formal disciplinary matter.

All technological resources developed by the College District employees, students, and contractors for use by the College District or as part of their normal employment activities are considered "works for hire." As such, the College District is considered the "author" and owner of these resources. Information regarding intellectual property rights may be found in the faculty and staff handbook.

[See CT]

DMCA DESIGNATED AGENT

Title II of the DMCA enables Internet service providers (ISPs), such as the College District, to limit liability for monetary damages related to copyright infringing activities of their users. Provisions within the legislation further protect educational institutions and limit liability for monetary damages caused by copyright infringing activities of their users. In order to comply with Title II of the DMCA, the College District designates the following individual as the DMCA designated agent to receive notices and claims from copyright owners about infringements:

Name: David Hoyt

Position: Chief Information Systems Officer

Address: 3452 Spur 339, McKinney, TX 75069

Telephone: (972) 599-3133

E-mail: dhoyt@collin.edu

Additionally, the College District shall maintain a prominent link on the information technology page of the College District website that provides access to this policy and a link to report DMCA notices or claims to the DMCA-designated agent.

VIRUSES

It is the responsibility of the user, to the best of his or her knowledge and ability, to ensure that any imported or exported executable code or data are free of any destructive code, such as a virus. To this end, best practices regarding safety precautions shall be taken by the user. The office of information technology shall be consulted for questions related to such precautions or information and protective software.

BACKUPS

It is the responsibility of the appropriate administrator or network administrator to ensure that appropriate procedures and resources are in place to backup data on a regular basis. Backups are to be stored in a location that is physically secure to protect the confidentiality of the data. It is the responsibility of the individual user to perform any actions necessary to comply with these procedures.

PHYSICAL SECURITY

Each user shall be responsible for the physical security of the technological and information resources to which he or she has been assigned (e.g., desktop computer, laptop computer, pager, cell phone, bar code, scanner, and the like). Administrators shall help to ensure physical security by instituting procedures for the use of locked doors and/or for the use of security devices made available by the College District for the protection of equipment. To avoid loss by fire or theft, backups of important data shall not be stored in the same location as the originals. Certain electronic information shall only be stored on the College District's network, including College District-approved and College District-contracted external sites such as publisher websites for a course offered by the College District. This electronic information includes:

1. Confidential information that is protected by FERPA;
2. Personnel records; and
3. Other materials commonly recognized or considered as sensitive or confidential.

Adequate power regulators and surge suppressors shall be used.

COLLEGE DISTRICT PROPERTY

Technology and information resources that are the property of the College District shall not be copied, altered, manipulated, trans-

ferred, retained, or removed from campus without written authorization from the appropriate administrator. The location of each physical resource shall be entered in the College District's capital equipment inventory system and updated as necessary.

PERSONAL USE OF COLLEGE DISTRICT TECHNOLOGICAL RESOURCES

Authorization for the personal use of College District technological resources by employees shall be determined on an individual basis by, and at the discretion of, the appropriate administrator. The use of the College District's technological resources, including the network, for a revenue-generating activity that benefits an individual employee shall be strictly prohibited. Personal telephones and data connections in student housing are considered to be part of the private residence. Student use of these and other College District technological resources that intrudes on general College District use or that uses significant resources is prohibited.

MISUSE OF TECHNOLOGICAL AND INFORMATION RESOURCES

The use of College District technological and information resources and the resources themselves shall not be abused in any way. Users shall not attempt to alter the restrictions associated with their accounts or to attempt to breach internal or external security systems. Moreover, users shall not impersonate other individuals or misrepresent themselves in any way when using College District technological resources.

Users of network resources are prohibited from engaging in any activity that is proscribed by federal and/or state law. In addition, the network shall not be used for criminal purposes such as posting another individual's credit card numbers or personal access codes. External networks, for example, NEXUS, the Internet, and bulletin boards shall also be used in an ethical, responsible, and courteous manner, and all users shall adhere to the policies of these services.

College District technological and information resources shall not be used in a manner that is invasive or that diminishes their efficiency. One example of such use involves the broadcast function. Although current technology enables users to broadcast messages to all members of the College District community simultaneously, the use of this technology is restricted to official College District activities. Any nonwork-related broadcasts of general interest to the College District community, such as birth and wedding announcements, shall be posted to the College District's general information e-mail folder. Notices involving monetary transactions or those that are inappropriate or illegal shall not be posted using College District technological or information resources as defined in this policy.

INAPPROPRIATE MATERIAL

Users are to comply with the College District's Core Values and exercise caution and good judgment in accessing material using College District network resources. Material that includes language and actions that would constitute a hate crime (such as language that is racist or anti-Semitic, and the like), fighting language, or visual material that creates a hostile working environment shall be accessed only for legitimate academic and administrative purposes. This material shall be not be accessed in an environment and in a manner that will negatively affect third parties (including printing such information on public printers or forwarding it to others without their consent).

Communications from users of College District technology resources shall reflect civility and the College District's Core Values, which include a passion for learning, service and involvement, creativity and innovation, academic excellence, dignity and respect, and integrity. Therefore, the use of College District technological resources for creating or sending nuisance, harassing, or pornographic materials or messages is prohibited. For the purpose of applying the College District's disciplinary policy, the determination of what is pornographic or what constitutes a hate crime, fighting words, or visual material that creates a hostile working environment is within the sole discretion of the College District.

REPORTING VIOLATIONS

Violations of this policy, including any violations of the DMCA, shall be reported to the appropriate supervisor, director, dean, DMCA-designated agent, or other responsible person. DMCA notices or claims of infringements shall be immediately sent to the DMCA-designated agent listed in this policy.

Depending on the nature of the violation, the appropriate administrator may include the responsible vice president, chief information systems officer, human resources officer, or internal auditor.

Alleged violations shall be investigated and, if substantiated, addressed in accordance with appropriate College District disciplinary processes for students and employees.

The College District shall consider the intent, effect, and seriousness of the incident in levying sanctions for violations of this policy. Any person who engages in any kind of computer or systems misuse as described in this policy may be subject to disciplinary action, including the loss of computer privileges, suspension, and/or termination from the College District, and appropriate criminal prosecution, if warranted, under the applicable state and/or federal laws. Whenever the College District deems it appropriate, restitution may be sought for any financial losses sustained by the College District or by others as a direct result of the misuse.

HEOA / DIGITAL COPYRIGHT COMPLIANCE

The Higher Education Opportunity Act of 2008 (HEOA) addresses, in part, unauthorized file-sharing, including, but not limited to, music, streaming, video, images, and other electronic data, using College District networks. To deter unauthorized file sharing on the its networks, the College District shall:

1. Disclose annually to all users information that explains unauthorized distribution, including file-sharing, of copyrighted materials may subject the individual to civil and criminal liabilities; an explanation of federal copyright law, including a summary of penalties for related violations; and the College District's policies and procedures regarding unauthorized file-sharing, including disciplinary actions that may be taken against students who engage in unauthorized distribution or illegal downloading using the College District's information technology systems.
2. Follow a plan to effectively combat unauthorized distribution using a variety of technology-based deterrents.
3. Offer and provide access to alternatives to illegal file-sharing and downloading.

COPYRIGHT COMPLIANCE ANNUAL DISCLOSURE

The College District shall require each user of its technology resources to annually read the copyright disclosure [see CR(EXHIBIT)] and submit an online affirmation that he or she has reviewed the disclosure and is aware of and familiar with the College District's policies and procedures regarding illegal distribution of copyrighted materials.

Additionally, during orientation activities, the College District shall provide all students a copy of the copyright disclosure [see CR(EXHIBIT)] and information regarding the legalities associated with peer-to-peer file sharing.

PLAN TO COMBAT UNAUTHORIZED DISTRIBUTION

The College District shall use a variety of capabilities and products from commercial vendors in order to:

1. Perform bandwidth shaping;
2. Conduct traffic monitoring to identify the largest bandwidth users; and
3. Reduce or block illegal file-sharing.

The College District shall investigate and respond to all submitted complaints of violations of the DMCA according to the reporting procedures noted above.

ALTERNATIVES TO ILLEGAL FILE-SHARING AND DOWNLOADING

The College District encourages all users of its technology resources to utilize free or commercial services that provide the user with a legal way to copy and use various types of digital content and ensures the use of electronic media is in compliance with federal copyright law.

EDUCAUSE, an information technology consortium in higher education, maintains a website of links to legal sources of online content at the following web address: http://www.educause.edu/legalcontent.