~~Board~~ Orientation

The Board and the District President ~~shall~~will provide an orientation for new Board members within the calendar year of their election to assist them in understanding the Board's function, policies, and procedures. Assistance given in the orientation of new Board members may include the following, as appropriate or available:

1. Selected materials on the responsibilities of being a contributing member of the Board.
2. Material pertinent to meetings and an explanation of its use.
3. Invitations to meet with the District President and other administrative personnel designated by the District President to discuss services the administration performs for the Board.
4. Access to a copy of the Board's policies and administrative regulations and other documents and information currently in use by other Board members.
5. Information regarding appropriate meetings and workshops.
6. A formal orientation on legal and budgetary oversight responsibilities of the Board.
7. Other information and activities as the Board or the District President deems useful in fulfilling the role of Board member.

The District President ~~shall~~will work with the Board to address the training needs of Trustees.

Cybersecurity Training

The District President or designee ~~shall~~will determine, from the list of cybersecurity training programs certified by the Department of Information Resources (DIR) and published to DIR's website, the cybersecurity training program to be used in the College District. The District President in consultation with the Board Chair may remove access to the College District's computer systems and databases for noncompliance with training requirements as appropriate.

The District President ~~shall~~will periodically require an internal review of the College District to ensure compliance with the cybersecurity training requirements.

Public Information Coordinator

The Chief Public Relations Officer or designee ~~shall~~will fulfill the responsibilities of the public information coordinator and ~~shall~~will receive, on behalf of Board members, the training specified by Government Code 552.012.

The Chief Student Success Officer ~~Senior Vice President~~ ~~shall~~will oversee the performance of records management functions prescribed by state and federal law:

- Records Administrator, as prescribed by Local Government Code 176.001 and 176.007 [See BBFA and CFE]
- Officer for Public Information, as prescribed by Government Code 552.201–.205 [See GCB]
- Public Information Coordinator, as prescribed by Government Code 552.012 [See BBD]

Local Government Records Act

The term "local government record" ~~shall~~will pertain to all items identified as such by the Local Government Records Act.

"Local Government Record"

Records Management Officer

~~The Dean of Admissions and District Registrar~~ The District Registrar or Manager of Records Systems ~~shall~~will serve as and perform the duties of the College District's records management officer, as prescribed by Local Government Code 203.023, and ~~shall~~will administer the College District's records management program pertaining to local government records in compliance with the Local Government Records Act.

Notification

The records management officer ~~shall~~will file his or her name with the Texas State Library and Archives Commission (TSLAC) within 30 days of assuming the position.

Records Control Schedules

The records management officer ~~shall~~will prepare and file records control schedules with the TSLAC that comply with the minimum legal retention requirements for local government records and ~~shall~~will prepare and file timely amendments to maintain compliance.

Website Postings

The College District's records management program ~~shall~~will address the length of time records will be posted on the College District's website when the law does not specify a posting period.

Records Destruction Practices

All local government records ~~shall~~will be considered College District property and any unauthorized destruction or removal ~~shall~~will be prohibited. The College District ~~shall~~will follow its records control schedules, records management program, and all applicable laws regarding records destruction. However, the College District ~~shall~~will preserve records, including electronically stored information, and suspend routine record destruction practices where appropriate and in accordance with procedures developed by the records management officer. Such procedures ~~shall~~will describe

the circumstances under which local government records scheduled for destruction must be retained. Notification ~~shall~~will be given to appropriate staff when routine record destruction practices must be suspended and when they may be resumed.

Training

The records management officer ~~shall~~will receive appropriate training regarding the Local Government Records Act and ~~shall~~will ensure that custodians of records, as defined by law, and other applicable College District staff are trained on the College District's records management program, including this policy and corresponding procedures.

TECHNOLOGY RESOURCES

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 will be permitted. Technological and information resources will 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 will be observed. Those who are authorized to access confidential files will respect the privacy rights of others and use data only for legitimate academic or administrative purposes.

All users of College District technology resources will 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 will determine and authorize the appropriate degree of access.

Users will implement best practices in taking precautions to prevent the unauthorized use of their access codes. In choosing access codes, users will 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 will be held accountable for their own actions performed under their access codes and will 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 will change it immediately upon becoming aware that said code has been compromised.

Users will not attempt to access, search, or copy technological and information resources without the proper authorization. No one will use another individual's account without permission, and active sessions will not be left unattended. Providing or using false or misleading information in order to gain access to technological and information resources will be prohibited. Users will 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 will 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 will 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 will 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, avoiding the use of portable storage devices (i.e., thumb drives), 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. If portable storage devices that contain confidential information must be used, the device must be encrypted. A justification must also be provided to the Chief Information Security Officer.

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 will 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 email 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 will not knowingly fail to comply with the copyright 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 will 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 will be reminded of the laws, and the software or licensing violations will be removed. A second violation will result in removing the software or licensing violations, retraining of the user in copyright procedures, and taking appropriate disciplinary action. A third violation will 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 will 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~~Stephens

Position: Chief Information Officer

Address: 3452 Spur 339, McKinney, TX 75069

Telephone: (972) ~~599-3133~~516-5037

Email: ~~dhoyt@collin.edu~~dsstephens@collin.edu

Additionally, the College District will 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 will be taken by the user. The office of information technology will 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 will 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 will 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 will not be stored in the same location as the originals. Certain electronic information will 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 will be used.

Ownership of College Data

The College District owns all data created and stored in college-owned and college-leased equipment, including cloud-based applications. Videos captured through cameras on campus are owned and managed by the Information Technology Department in compliance with college policies and records retention requirements.

[See CHA(LOCAL) for Vehicle Dash Camera and Police Body Camera video requirements]

College District Property

Technology and information resources that are the property of the College District will not be copied, altered, manipulated, transferred, retained, or removed from campus without written authorization from the appropriate administrator. The location of each physical resource will 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 will 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 will 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 will not be abused in any way. Users will not attempt to alter the restrictions associated with their accounts or to attempt to breach internal or external security systems. Moreover, users will 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 will 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 will also be used in an ethical, responsible, and courteous manner, and all users will adhere to the policies of these services.

College District technological and information resources will 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. Notices involving monetary transactions or those that are inappropriate or illegal will 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 will be accessed only for legitimate academic and administrative purposes. This material will 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 will 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, will be reported to the appropriate supervisor, director, dean, DMCA-designated agent, or other responsible person. DMCA notices or claims of infringements will 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 officer, human resources officer, or internal auditor.

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

The College District will 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, in-

cluding 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 its networks, the College District will:

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 will 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 will 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 will 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 will 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[1] to legal sources of online content.

Access by Individuals with Disabilities

The District President or designee will develop procedures to ensure that individuals with disabilities have access to the College District's electronic and information resources similar to individuals without disabilities.

Drones

The flying of drones over or from sites on College District property or as part of the College District's administrative, academic, or research program is permitted only in accordance with law and College District regulations.

---

[1] EDUCAUSE: http://www.educause.edu/legalcontent

Each employee ~~shall~~will meet the professional development standards described by the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC) as well as any professional development required of the employee by state or federal law or administrative regulations.

Each employee ~~shall~~will seek approval prior to pursuing professional development in accordance with administrative regulations.

Cybersecurity Training

The District President or designee ~~shall~~will determine, from the list of cybersecurity training programs certified by the Department of Information Resources (DIR) and published to DIR's website, the cybersecurity training program to be used in the College District. The District President ~~shall~~will verify and report to DIR, in the form required by DIR, the compliance of each employee required to complete the program. The District President may remove access to the College District's computer systems and databases for non-compliance with training requirements as appropriate.

The District President ~~shall~~will periodically require an internal review of the College District to ensure compliance with the cybersecurity training requirements.

At-Will Employees

At-will employees may be dismissed at any time for any reason not prohibited by law, including, but not limited to, reasons for disciplinary action set out in Board policy or for no reason, as determined by the needs of the College District. For example, at-will employees may be dismissed at any time for the grounds for disciplinary action specifically listed in DMAA. At-will employees who are dismissed may request review of that decision through DGBA(LOCAL) and will receive pay through the end of the last day worked.

Severance Benefits

The College District must continually assess its operations, evaluate personnel, and allocate staffing wisely to operate efficiently and effectively. When a position(s) or an individual's employment with the College District is no longer supportable, the College District will take appropriate action.

In the case of an organizational change or position elimination, reasonable effort will be made to reassign displaced employees to available positions. If these efforts are not successful, severance benefits may be provided to ease the transition from employment. Exceptions to this severance benefits policy may be granted by the District President.

Eligibility

Under this policy, regular full-time noncontract staff who have completed their 90-day probationary period are eligible for severance benefits if:

1. The position they hold is eliminated and reassignment to a comparable or available position is not offered;
2. They are part of an early exit incentive program; or
3. Their employment is otherwise involuntarily terminated.

Employees within their 90-day probationary period, temporary employees, adjunct faculty, part-time employees, grant employees (unless allowed under the applicable grant), and contract employees are not eligible for severance benefits under this policy.

In the event of a position elimination or other organizational change, the College District will attempt to provide reasonable advance notice to these employees, when feasible.

Severance Pay

Eligible employees will be provided all benefits and compensation normally due to separating employees and COBRA or other insurance continuation options, if applicable.

Subject to receipt by the College District of a fully executed release of all claims in a form acceptable to the College District, severance-eligible employees may also be provided:

1. Two calendar weeks of pay at the final base salary rate as notice or pay in-lieu-of notice;
2. One week of base pay as severance for each year of full-time service with the College District, generally to a maximum of six calendar weeks, which will be provided at the final base salary rate (excluding any other forms of final or additional pay due to the employee under applicable law); and
3. Outplacement assistance and career counseling services of the Human Resources department, if available.

Severance pay will not exceed the District President's contracting authority as set by Board policy CF.

Distribution of Severance Benefits

If pay-in-lieu of notice is provided, the employee will remain on the payroll on administrative leave until that period is exhausted. Severance pay will be distributed as a lump sum payment that will be issued after the employee signs the release and any required notice period is exhausted.

Reemployment

Employees who have received severance pay benefits are not eligible for reemployment with the College District until the notice period and severance pay distribution period have been fully exhausted or an agreement to reimburse severance pay for future weeks has been executed.

Resignation

The District President ~~or designee~~ is authorized to accept the resignation of an at-will employee at any time. The District President may delegate to other administrators the authority to accept a resignation of an at-will employee. The College District has the sole discretion to designate a resigning employee's earlier final day at work, whether or not the intended notice period has been fully satisfied. Once submitted and accepted, the resignation of an at-will employee may not be withdrawn without the consent of the District President or designee. [See DMD]