

BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

SUBJECT: *Information Resources Acceptable Use, Security and Copyright Infringement*

EFFECTIVE DATE: July 16, 2020

BOARD POLICY REFERENCE: CR, CS, and CT

PURPOSE

To ensure clear guidance on the use of Blinn College District Information Resources and its application to copyright law for employees, students, authorized Users, and the community. This regulation applies to all information technology resource and electronic media Users, including but not limited to administrators, faculty, staff, students, Board members, agents, volunteers, vendors, and the community, both on campus and at remote sites. All information resource and electronic media Users shall comply with this procedure.

AUTHORITY

The Dean of Academic Technology Services and the Director of Administrative Computing are responsible for Blinn College District Information Resources and electronic media. Blinn College District reserves the right to systematically and randomly audit the contents of all electronic media to determine adherence to policies and/or procedures and, if requested, to provide material to the state auditors for audit purposes. In the event that any Blinn College District information technology resource user leaves, resigns, or in any way concludes his or her relationship with Blinn College District for whatever reason, access to all Information Resources, including voice mail and e-mail services, will be terminated immediately unless continued access is authorized and approved by the appropriate parties.

DEFINITIONS

- Information Resources - includes all forms of the acquisition, processing, storage, and dissemination of vocal, pictorial, textual, and numerical information by electronic-based computing or telecommunications.
- Electronic Media - includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing Web sites, editorial comments posted on the Internet, and social network sites. Electronic media also includes all forms of telecommunication, such as landlines, cell phones, and Web-based applications.
- College District Data - All data or information held on behalf of the Blinn College District, created as result and/or in support of College District business, or residing on College District Information Resources, including paper records.
- Confidential Data or Confidential Information - All College District Data that is required to be maintained as private or confidential by applicable law.
- Users - include anyone authorized to access information resources and/or electronic media owned or operated by Blinn College District.
- Copyright Infringement - is the unauthorized use of copyrighted material in a manner that violates one of the copyright owner's exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works that build upon it.
- DMCA (Digital Millennium Copyright Act) - is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO).

USER RESPONSIBILITIES

Access to information technology resources and/or electronic media owned or operated by Blinn College District is a privilege granted to authorized Users. Users are responsible for:

- Reviewing, understanding, and complying with all College District regulations, policies and/or procedures related to access, use, and the security of College District Information Resources and/or electronic media;

- Adhering to all hardware and software license agreements that are in force on any College District system, network, or server;
- Asking system administrators or data owners for clarification of access and acceptable use issues not specifically addressed in College District regulations, policies and/or procedures; and
- Reporting possible violations to the appropriate parties.
- All activities conducted using the User's password or other credentials.
- Report as soon as possible the loss of Information Resources to their supervisor and other appropriate employee including the CISO and police.

EMPLOYEE USAGE

Blinn College District's Information Resources are made available to employees to assist with fulfilling their job responsibilities. Employees shall be held to the same professional standards in their use of Blinn College District electronic media as they are for any other public conduct. If an employee's use of electronic media violates state or federal law or College policy and/or procedure or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. Violations of local, state, and federal laws will be reported to appropriate authorities for investigation and prosecution.

STUDENT USAGE

Blinn College District's Information Resources are made available to students to further the educational mission of the College. To ensure availability and reasonable levels of service, the Users must exercise responsible, ethical behavior. The misuse of Information Resources by a few can result in degraded performance for all Users and interfere with legitimate academic endeavors. Failure to follow this procedure can result in suspension or termination of access to Blinn College District's Information Resources and/or electronic media, as well as, other disciplinary actions by the College. Blinn College District reserves the right to investigate any unauthorized or improper use of College District Information Resources. The appeal of any suspension or termination of access or other disciplinary actions shall be governed by the due process procedures outlined in Board Policy and the College Catalog. Violations of local, state, and federal laws will be reported to appropriate authorities for investigation and prosecution.

COMMUNITY AND OTHER AUTHORIZED USAGE

Blinn College District's Information Resources are made available to community and other authorized Users for general use consistent with College District activities. The misuse of Information Resources by community and other authorized Users can result in limited or terminated access. Violations of local, state, and federal laws will be reported to appropriate authorities for investigation and prosecution.

GENERAL GUIDELINES

- Blinn College District Information Resources and/or electronic media may not be used: to interfere with normal operations and other Users; to violate city, state, and/or federal laws; to damage or impair College resources; for commercial use; and/or for more than occasional incidental personal communication.
- All reasonable efforts shall be made by Users to prevent unauthorized access to the Blinn College District information technology systems. Users shall be responsible for protecting the confidentiality of their password. Users shall be responsible for changing their password if it becomes compromised.
- Users shall minimize the electronic exchange of large files not consistent with College District business.
- No effort will be made to guarantee privacy of electronic media other than to limit access to College District employees, students, and authorized Users only. Messages which are returned as undelivered or improperly addressed will be reviewed as part of the ongoing operation of the e-mail system.
- Electronically stored information, including electronic information archived on backup tapes, is subject to subpoena by civil and criminal courts, as well as, some open records requests.
- The following activities are not allowed: non-business file sharing; spamming; chain mail; downloading or installing unauthorized software or other applications; unauthorized access, removal or modification of College

District Data, applications or equipment; unauthorized use of network packet ‘sniffers’ or packet analyzers; unauthorized installation of routers, switches, hubs, or wireless access points; unauthorized scanning systems to find running services and vulnerabilities; and unauthorized running of Web, proxy, or e-mail servers from computers connected to Blinn College District information technology infrastructure.

- Whenever possible Users shall store confidential information or other information essential to the mission of the College District on centrally managed servers or storage systems and not on individual computers or storage drives.
- Users shall access College District Data only to conduct College District business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing College District Data in accordance with College District’s Records Retention Policy and Records Management Guidelines.
- Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official College District duties.
- When a user must create or store confidential information or essential College District Data on local hard drive or portable device such as a USB drive, laptop, tablet or smart phone the user must ensure the data is encrypted in accordance with College District encryption regulations.
- The following College District Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver’s License Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual’s financial accounts; bank routing numbers; and other College District Data about an individual likely to expose the individual to identity theft.
- Users who store College District Data using commercial cloud services must use services provided or sanctioned by College District, rather than personally obtained cloud services.
- Devices determined by College District to lack required security software or to otherwise pose a threat to College District Information Resources may be immediately disconnected by the College District from a College District network without notice
- Users are to use College District provided email accounts, rather than personal email accounts, for conducting College District business.
- All electronic devices including personal computers, smart phones or other devices used to access, create or store College District Information Resources, including email, must be password protected in accordance with College District requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.
- College District Data created or stored on a User’s personal computers, smart phones or other devices, or in data bases that are not part of College District’s Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to College District Information Resources
- College District issued mobile computing devices must be encrypted
- Any personally owned computing devices on which Confidential College District Data is stored or created must be encrypted.
- College District Data created and/or stored on personal computers, other devices and/or non- College District Data bases should be transferred to College District Information Resources as soon as feasible.
- Unattended portable computers, smart phones and other computing devices must be physically secured.
- All remote access to networks owned or managed by College District must be accomplished using a remote access method approved by the College District, as applicable.

COPYRIGHT INFRINGEMENT PROCEDURES DISCLOSURE

Blinn College District shall annually disclose that unauthorized distribution of copyrighted material may be illegal, as well as, the Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws:

- Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.
- Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than \$750 and not more than \$30,000 per work infringed. For "willful" infringement, a court may award up to \$150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.
- Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

DMCA NOTICES/ILLEGAL DOWNLOADING AND DISTRIBUTION STUDENTS

The procedure to effectively combat the illegal downloading and distribution of copyrighted material for Blinn College District is as follows:

- Locate and block access of the source
- Send notice to the student responsible
- Report second occurrence to the Vice Chancellor, Student Services for student discipline
- To have access re-established, the user must acknowledge receipt of complaint and copyright information and/or successfully complete any requirements set forth by the Blinn College District Student Discipline Process

EMPLOYEES

- Locate and block access of the source
- Send notice to the employee responsible, as well as, their immediate supervisor
- Report second occurrence to the appropriate supervisor for employee discipline
- To have access re-established, the user must acknowledge receipt of complaint and copyright information and/or successfully complete any requirements set forth by the Blinn College District Employee Discipline Process

COMMUNITY AND OTHER AUTHORIZED USERS

- Locate and block access of the source
- Send notice to the user responsible
- Report second occurrence to the appropriate authorities for investigation and action

DETERRENTS

Blinn College District utilizes two types of deterrents for the illegal distribution of copyrighted material:

- Bandwidth shaping
- Vigorous program of accepting and responding to DMCA notices

DMCA AGENT

Blinn College District shall designate a DMCA agent to receive notifications of Copyright Infringements Claims. The Blinn College District DMCA agent is:

Mr. Brad Rowland
DMCAagent@blinn.edu
 979-830-4020