Clint Independent School District
Employee Acceptable Use Policy

Foreword
The Employee Acceptable Use Policy (AUP) is designed to align with law and District policy. The AUP is not meant to be a complete statement of all policies, procedures, or rules in any given circumstance. In case of conflicts between board policy and any AUP provision, the district will follow board policy. The AUP is updated periodically; however, policy adoption and revisions may occur throughout the year. The district encourages employees to stay informed of proposed policy changes by attending board meetings and reviewing communications explaining changes in policy or other rules and provisions. The district reserves the right to modify the AUP at any time. Notice of revisions will be provided as is reasonably practical.

Mission
Clint ISD is a District of Innovation and strives to provide educators and students the best most up to date advancements in computing and technological resources for education. While online tools provide a wealth of learning opportunities and supports, they also come with a certain level of risk. The AUP helps ensure that employees cannot use district-issued technology to access inappropriate content or expose themselves to cyber threats.

Notice of Responsibility
This document is an agreement establishing specific requirements for the use of all computing devices, network resources, other technology equipment/devices, hardware, software, and cloud computing resources collectively referred to as **District Technology Resources** used to access technology owned, leased or managed by the Clint Independent School District hereinafter referred to as "the District".

All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's Technology Resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines for the duration of their employment with the District. The Employee shall adhere to this Agreement upon assignment of any current or new program, device, network, or technology to be used by the employee. Acknowledging receipt of the Employee Handbook is acceptance of this Employee Technology Acceptable Use Policy. **The Employee must notify their direct supervisor and the Chief Technology Officer of any loss, theft, damage, or security breach of District technology within 24 hours**. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District. [CQ (LOCAL)] The District reserves the right to seek monetary restitution from the Employee as allowed by state and federal law in the case of loss or damage to a District device used by the employee.

Purpose of District Technology Resources
The District Technology Resources support the school district's mission of educating our students in a safe, supportive, academic environment. Use of these resources is extended to employees to promote this mission. As a user of these resources, you, the Employee, have access to valuable equipment, sensitive data, confidential information excepted under the Texas Public

Information Act, confidential information under the Family Educational Rights and Privacy Act (FERPA), and to internal and external networks. Consequently, it is important for all employees to act in a responsible, ethical, and legal manner when accessing or using District Technology Resources.

Scope
The Employee Acceptable Use Policy applies to all users of technology resources owned, leased or managed by the District, as well as personally owned technology devices connected to the District network and applications. Technology resources include all District-owned, leased, licensed, or managed hardware and software and use of the District network via a physical or wireless connection, regardless of the ownership of the device connected to the network.

Bring Your Own Device (BYOD)
Unless approved by a supervisor and the Chief Technology Officer employees are not permitted to bring their own computing devices to school, including tablets, laptops, printers, or other computing devices. Employees are prohibited from connecting personal electronic devices to the district's networks. All employees must use district-issued devices for instructional and administrative functions. This policy helps protect our network from security risks and ensures that all employees have consistent access to the educational tools and resources provided by the district. In addition, the district does not provide support for the use employee personal assets (such as home printers or home Internet access) with district assets.

Personal Cellular Devices
Employees may bring and use personal cellular devices to work but are not permitted to use WIFI on their cellular devices while at a campus or non-instructional facility. Employees that use personal cellular devices for work must adhere to these additional requirements:

- The employee must setup a device password, pin, gesture, or biometric security policy to restrict unauthorized access to the device.
- The device must always remain locked by security measures listed above when not in use.
- The employee must install and accept District authorized device policy apps as a security measure to secure the employees device and data in case of loss of theft.

Your Rights and Responsibilities
As a user of District Technology Resources, you are permitted to use technology and information assets that are required to perform work related duties, including access to certain computer systems, servers, software and databases, phone, smartphone, laptop, computers, email and voicemail systems, and the Internet. The District makes reasonable efforts to protect users from abuse and intrusion by others sharing these resources.

In turn, you are responsible for knowing and understanding the policies of the District that apply to the appropriate use of technology resources. You are responsible for exercising good judgment regarding the use of District technological and information resources and remaining in compliance with all applicable policies.

Employees shall abide by the following Acceptable Use Policies:

I. Employees shall adhere to the Principle of Least Privilege and only use the computers, computer accounts, and computer files for which you have authorization to access and resources needed to perform your stated job function.

II. Employees shall comply with the Family Educational Rights and Privacy Act (FERPA) concerning the confidentiality of student information.

III. Employees shall adhere to the District's password standards and take all precautions necessary to protect your account and passwords to secure resources against unauthorized use or access. Users shall not disclose their passwords to others.

IV. Employees are individually responsible for appropriate use of all resources assigned to them, including but not limited to accounts, passwords, a computer, other devices, network resources, software, and hardware.

V. Employees shall not use District issued credentials (email accounts) to conduct personal business or to register or log on to suspicious or illicit sites which could compromise their accounts or pose un-necessary security risks.

VI. Employees shall not allow any unauthorized person to access District Technology Resources.

VII. Employees shall use appropriate password protections for sensitive or confidential files in addition to an appropriate message encryption when transmitting sensitive data via email systems or file sharing.

VIII. Employees shall limit the sharing of sensitive data to users both internal and external to only the data necessary and to only those users that have a legitimate business purpose to receive the data.

IX. Employees shall utilize an appropriate password scheme, access restriction list, and or encryption to control the sharing of all data, regardless of sensitivity level, and will revoke access immediately concluding the academic or business activity.

X. Employees must respect the integrity of computing systems and abide by existing federal and state laws regarding electronic communication. This includes accessing secure and/or confidential information such as but not limited to grades, attendance and demographic information stored on District Technology Resources without authorization, divulging passwords, causing system malfunction, developing programs that harass other users or attempting to infiltrate a computing system or data, and deliberately degrading or disrupting system performance. These actions may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws.

XI. Employees shall not attempt to gain unauthorized access to the District's Technology Resources or any other system or go beyond their authorized level of access. This prohibition includes attempting to log in through another account or accessing or attempting to access another person's files without authorization.

XII. The District shall be bound by contractual and licensing agreements with regard to third-party resources. Employees are expected to comply with all such agreements when using such resources.

XIII. Employees shall comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

XIV. Employees shall conduct themselves in a manner that is appropriate and proper as representatives of the school district community.

XV. Any security issues or potential security issues discovered shall be reported to or his/her direct supervisor, the Chief Technology Officer, and Cybersecurity Coordinator as soon as possible **not to exceed 24 hours** for follow-up investigation.

Employees shall abide by the following Unacceptable Use of District Technology Resources:

I. Employees shall not use the District's Technology Resources to access, send, receive, view or download any obscene material or child pornography. No employee shall access, send, receive, view or download any material that is harmful to minors. An employee who gains access to any inappropriate material is expected to discontinue the access immediately and to report the incident to his or her supervisor and the Chief Technology Officer. (Refer to policy CQ)

II. "Harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

b. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

c. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

47 U.S.C. 254(h)(7)(G); 20 U.S.C. 7131(e)(6)

III. Employees shall not attempt to bypass any security control or technology protection measure unless you have been specifically authorized to do so by the Superintendent or his/her designee.

> "Technology protection measure" means a specific technology that blocks or filters internet access to the material covered by a certification described at Certifications to the FCC, below, to which such certification relates.
>
> 47 U.S.C. 254(h)(7)(I)

IV. Employees shall not attempt to access or provide resources to access restricted portions of the network, an operating system, security software, or other administrative applications without appropriate authorization by the system owner or administrator.

V. Employees shall not engage in deliberate activity to degrade the performance of technology resources, deprive an authorized user access to District Technology Resources, or circumvent District physical and cyber security measures. Any activity that does not fall within the mission of this AUP and which slows the system or exceeds resources is strictly prohibited. Examples of activities that degrade or tax system resources include, but are not limited to, sending mass unsolicited and unwanted email (“Spam”), attaching large files to email, flooding servers, or exceeding storage limits.

VI. Employees shall not store, share, process, analyze, or otherwise communicate confidential information, data, or files using unauthorized mediums, applications, or infrastructure, including but not limited to cloud storage, personal electronic storage, or unauthorized applications.

VII. Employees shall not use the District’s Technology Resources to send, receive or download any copyrighted material for which you do not have a license or are entitled to. Employees shall not receive or transmit any illicit license, code, key, or use of devices or technologies used to circumvent copyright protection. (See Policies CY and CQ)

VIII. Employees shall not engage in any illegal act, or in an act in furtherance of an illegal act. Employees shall not transmit any material that is in violation of any federal or state law. This includes, but is not limited to, student or other confidential information, copyrighted material, threatening or obscene material, or computer malicious software. Other examples of such illegal acts include but are not limited to using the District's Technology Resources to arrange the sale or purchase of contraband, illicit drugs, engaging in criminal activity, transferring stolen financial information, gambling, crypto mining, contract violations or threatening the safety and wellbeing of another individual.

IX. Employees shall not use District computing services, networks, and equipment for political purposes, personal economic gain, or use in any way that is in violation of District policies.

X. Employees shall not use the District's Technology Resources to annoy, harass, threaten, bully, or stalk any other person.

XI. Employees shall not attack, flood, broadcast storm, or engage in any other behavior that disrupts the District's Technology Resources or an external computer, system, or network.

XII. Employees shall not use another person's account, password, or ID card or allow another user to use their own account, password, or ID. If an employee's account has been compromised or suspected to be compromised, employees must change their passwords immediately.

XIII. Employees must adhere to Multi-Factor Authentication, 2-Step Verification, and any other policies and cybersecurity measures designed to protect and keep and keep an employee's account secure from unauthorized access.

XIV. Unless authorized to do so by a supervisor, employees shall not log on or attempt to log on to the District's Technology Resources impersonating another District employee, or a student.

XV. Posting or transmitting pictures of students or other individuals without obtaining prior permission from all individuals depicted or from parents of depicted students who are under eighteen years of age is prohibited.

XVI. Unless otherwise authorized to do so by a supervisor for an instructional related activity or legitimate business purpose, employees may not use the District's Technology Resources to engage in any form of real-time online chatting. Examples of software and websites designed for real-time chatting include, but are not limited to, X (formally known as Twitter), Facebook, Instagram, WhatsApp, Snapchat, Kik, Viber, Discord.

XVII. Employees shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language. Employees shall not engage in personal attacks, including prejudicial or discriminatory attacks. Restrictions against inappropriate language apply to public messages, private messages and material posted on the Internet.

XVIII. Employees shall not engage in any conduct that causes harm to others. Examples of such conduct include engaging in fraud or knowingly or recklessly posting false or defamatory information about a person or organization.

XIX. Unless authorized to do so employees may not stream video or music content that is unrelated to an educational activity or district business.

XX. Employees shall not use District Technology Resources for purposes of sharing confidential student information with others, including District employees, who do not have a legitimate educational interest in that student.

XXI. Employees shall not use District Technology Resources in a way that is considered offensive, defamatory, or obscene, including, but not limited to: sexual images, jokes, and comments; racial or gender-specific slurs, images, or jokes; or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin or ancestry, or any other category protected by federal, state, or local laws.

XXII. Employees shall not deliberately attempt to disrupt the District's Technology Resources performance, destroy or alter other people's data by spreading or using Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, trojan viruses, spyware, adware, and ransomware.

Privacy and Personal Rights

- Access to and monitoring of the District's network, technology resources, equipment, devices and information systems shall be performed by designated personnel at any time to ensure appropriate use under the law, board policy, and administrative procedures.
- All users of the District's network and computing resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without the written permission of the appropriate data owner.
- Be professional and respectful when using District Technology Resources to communicate with others. The use of computing resources to libel, slander, or harass any other person is a violation of District policy and will subject the offending party to disciplinary action.
- The District reserves the right to monitor, access and review information transmitted on the District Technology Resources at any time to ensure the security of information assets. These include investigating performance deviations and system problems (with reasonable cause) to determine if an individual is in violation of this policy or, as may be necessary, to ensure that the District is not subject to claims of illegality or misconduct.
- Electronic mail transmissions and other use of the District Technology Resources by employees shall not be considered private.

Compliance

Employees found to be in violation of this Agreement will have his or her privileges to District Technology Resources denied and shall be subject to disciplinary action up to and including termination. The employee in whose name a system account and/or computer hardware is issued will always be responsible for its appropriate use. Violations of applicable state and federal law, including the Texas Penal Code Computer Crimes Chapter 33, may result in criminal prosecution, as well as disciplinary action by the District. The District cooperates fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. In addition, contents of e-mail and network communications are governed by the Texas Public Information Act, and therefore, may be subject to public disclosure as

required by law. Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus or district administrator, will be considered a violation of policy and subject to disciplinary action.

THIS ACCEPTABLE USE POLICY DOCMENT IS FOR YOUR INFORMATION.

ACKNOWLEDING RECEIPT OF THE DISTRICT EMPLOYEE HANDBOOK IS ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS ACCEPTABLE USE POLICY.

THIS FORM DOES NOT NEED TO BE TURNED IN

I understand and will abide by the Clint ISD Employee Acceptable Use Policy for District Technology Resources.

I understand that my computer use is not private and that the district will monitor my activity on the computer system. I have read the District's electronic communication system policy and administrative regulations and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access and shall be subject to disciplinary action up to and including termination.