Clint Independent School District
Student Acceptable Use Policy

Foreword

The Student 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 parents 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 students cannot use district-issued technology to access inappropriate content, expose themselves to cyber threats, or simply distract themselves from their schoolwork (via gaming, streaming shows or movies, or using social media).

Purpose

The purpose of this policy is to outline acceptable conduct by students in reference to the use of the district's technology resources, systems, and data. This Policy governs the use of all district computing system resources and data owned, leased, in the possession of, or otherwise provided by the district. Such resources include but are not limited to computing systems, hardware, software, firmware, structured and unstructured data, networks, and Internet access, collectively referred to as **District Technology Resources**.

Bring Your Own Device (BYOD)

Students are not permitted to bring their own computing devices to school, including tablets, laptops, or other computing devices.
Students may bring cellular devices to school but are not permitted to use WIFI on their cellular devices while at school. (See **Electronic Devices and Technology Resources (All Grade Levels) Possession and Use of Personal Telecommunications Devices, Including Cell Phones, and Other Electronic Devices** for more information.)

Availability of Access

Access to the District's Technology Resources, including the Internet, shall be made available to students primarily for instructional and administrative purposes and in accordance with administrative regulations. The District's Technology Resources shall be used for educational purposes, preparing students for a technology-oriented society, the job market, promoting educational excellence, and conducting official District business. The approved usage of the district's technology and computing resources include, but are not limited to, facilitating innovative instruction for students, sharing educational resources, educational research, access to

a wide range of information related to academics and enrichment, and the ability to communicate and collaborate with others throughout the world. To optimize performance of the District's technology and computing resources, its usage requires efficient, ethical, and legal utilization. Use of the District's Technology Resources must be in support of the student education and preparation for college, career or military readiness and must support the mission of the District in accordance with all Board Policies and school regulations.

Monitored Use

Electronic mail transmissions and other use of the District's Technology Resources by students, employees, and members of the public shall not be considered private. Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

Acceptable Use

Access to the District's Technology Resources is a privilege, not a right. 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.

Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct.] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Students shall abide by the following Acceptable Use Policies:

I. Duty to Maintain Password Confidentiality
Students are responsible for the use of their individual accounts and passwords. Students should take all precautions to prevent others from being able to access their accounts. Except for a parent or guardian students shall not disclose their passwords to others. No staff member from Clint ISD will ever ask a student for his or her password.

II. Duty to Maintain Account Protection
Students shall not use Clint ISD issued email account or credentials to register or log on to suspicious, illicit, or non-district sanctioned websites which could compromise their accounts. Students may not user their district issued account for personal use.

III. Duty to Report Security Issues
Students shall immediately notify a teacher or staff member if they have identified a possible security issue.

IV. Respect Resource Limits
Students shall use the District's Technology Resources only for educational, supplemental, or enrichment activities. 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 slow the system are but not limited to, sending mass unsolicited and unwanted email

(spam); attaching large files to email, attempting denial of service attacks, flooding servers, streaming audio or video, downloading or uploading non-educational content or copyrighted material to local hard drives or cloud storage.

V. Duty to Report Abusive Behavior

Students shall promptly disclose to a teacher or other staff member any message they receive that is inappropriate, offensive, cyberbullying or makes them feel uncomfortable.

VI. Personal Safety

Students shall not meet or agree to meet in person anyone they have met online via the Internet. Students shall not share or disclose any personal or personal identifiable information online.

VII. Commercial/Political Activity

Students shall not distribute advertisements, solicitations, commercial documents of any kind, or political materials via the District's Technology Resources.

VIII. Ecommerce

Students shall refrain from engaging in commerce via District Technology Resources. Any expense incurred because of Internet use is the responsibility of the student/parents.

IX. Personal Conduct and Accountability

Students are personally responsible for their actions and any actions in which an audit reveals the use of their issued account in accessing and utilizing the District's Technology Resources.

X. Digital Citizenship

As part of the Internet Safety Plan all students shall complete digital citizenship training annually and are expected to practice good Digital Citizenship. Training includes but is not limited to:

1. Being courteous and respectful in all communications
2. Practicing appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms
3. Cyberbullying awareness and response
4. Cybersecurity Awareness and response

XI. Care and Return of Assets

Clint ISD may make technology equipment available for student checkout and use. Upon availability, the campus may checkout a device to engage students in 21st century learning opportunities. The "device" may include, but is not limited to calculators, tablets, laptops, hotspots, chromebooks, chargers and cables.

To checkout a device, A Technology Device Agreement must be completed by the student and parent/guardian every year upon registration agreeing to abide by each item below. "We" includes the student and parent/guardian, agree to, and shall, exercise reasonable care and judgment while using the device daily for instructional use as needed.

1. We understand the device and any other peripherals (charger) are the property of the Clint ISD. We will return the device(s) in the same condition, less reasonable wear and tear. The device will be returned to the originating Clint ISD campus as requested by the campus administration or Clint ISD designee.

2. In case of a device malfunction, we must notify the campus administration, librarian, and campus technology contact immediately and arrange to return the device for inspection. The device(s) are not to be taken to any outside entity for repairs or replacements of any kind. Personal data/files should not be stored on the device and will be erased upon return of the device.

3. If the device is lost or stolen, we will complete a police report with the proper authorities such as the El Paso County Sherriff's Department, Horizon Police Department, the El Paso Police Department, or Clint ISD Security Department within twenty-four (24) hours and provide a hard copy of report, a case number, and any other information to the campus administration or Clint ISD designee. We understand that the device may have been purchased with state and/or federal funds and thus, may be subject to investigation in case of loss theft. The district is also entitled to file a police report on behalf of the student and parent/guardian if no action was taken in a timely manner or there was no cooperation on behalf of the parent/guardians. **It is also understood that we will be personally responsible for the replacement cost of the device.**

4. Parents/student will be responsible for any damage due to accidental, negligent, or malicious treatment of the device. The cost to repair or replace the device with a new one will be determined and assessed by the campus administration CISD designee. Each student, or the student's parent or guardian, is responsible for all instructional materials and technological equipment not returned in an acceptable condition by the student. A student who fails to return in an acceptable condition all instructional materials and technological equipment forfeits the right to free instructional materials and technological equipment until all instructional materials and technological equipment previously issued but not returned in an acceptable condition are paid for by the student, parent, or guardian.
   (See Texas Education Code 31.104).

A Student who receives data processing equipment from a district under these provisions shall return the equipment to the district not later than the earliest of:

1. Five years after the date the student receives the equipment;
2. The date the student graduates;
3. The date the student transfers to another district; or
4. The date the student withdraws from school.

(See Policy CQC)

Note: Students in grades 5, 8, and 12 must return all district assets issued to them at the end of the school year. Returning Clint ISD students will receive devices issued to them from the home campus upon registration at grades 6, and 9.

Unacceptable Use

Students are prohibited from using the District's Technology Resources to engage in any behavior that is inconsistent with the District's Vision, Mission, and Goals.

Students shall abide by the following Unacceptable use of District's Technology Resources

I. Viewing or Transmitting Obscene Material

Students shall not use the District's Technology Resources to access, send, receive, view or download any obscene material or child pornography. No student shall access, send, receive, view or download any material that is harmful to minors. A Student who gains access to any inappropriate material is expected to discontinue the access immediately and to report the incident to a district staff member. (Refer to policy CQ)

"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)

II. Technology Protection

Disabling, attempting to disable or bypass a Technology protection measure is prohibited.

"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)

III. Infringing Others' Copyrights

Students shall not use the District's Technology Resources to send, receive or download any copyrighted material for which they do not have a license or are entitled to. Students 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)

IV. Engaging in Illegal Activity Knowingly

Students shall not engage in any illegal act, or in an act in furtherance of an illegal act. Students 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, contract violations or threatening the safety and wellbeing of another individual.

V. Cyberbullying and Harassment

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

VI. Network Systems Misuse

Students shall also 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.

VII. User Account Misuse

Students shall not use another person's account, password, or ID card or allow another user to use their own account, password, or ID.

VIII. Chatting & Messaging

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

IX. Using Inappropriate Language

Students shall conduct themselves in a manner that is appropriate and proper as representatives of the school district community. Students shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language. Students 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.

X. Engaging in Wrongful Conduct

Students 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.

XI. Committing Plagiarism

Students shall not use the District's Technology Resources to take the ideas or works of others and present them as if they were original. Students shall use proper methods of attribution and citation.

XII. Impersonation

Students may not log on or attempt to log on to the District's Technology Resources impersonating a District staff member, another student, or any individual other than the Student.

XIII. Use of Pictures

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.

XIV. Streaming Services

Students may not access online videos, music, or streaming content that is unrelated to an educational activity or district business.

XV. Harassment and Discrimination

Students may not use or access the District Technology Resources in a manner that violates the district's prohibitions against harassment and discrimination. Students may not engage in sexual harassing conduct or use any language of a sexual or otherwise objectionable nature in public or private message.

XVI. Improper Use

Students shall not use District Technology Resources to access or explore online content that does not support the curriculum, is unrelated to school activities and/or is inappropriate for school assignments. Students may not cause congestion on the network or interfere with the work of others. Students may not obtain copies of or modify files, data, or passwords belonging to other Students on the network without authorization.

XVII. Hacking & Unauthorized Access

Students 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. Students 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.

XVIII. Spreading Malware/Destroying Data or Equipment

Students 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.

XIX. Protection of Resources and Care of Assets

Students are responsible for protecting the District's Technology Resources. Any attempt to harm or destroy District equipment, systems or data, or to harm or destroy the data of another is prohibited. Students are expected to care for district assets issued or used by students. Parents/student will be responsible for any damage due to accidental, negligent, or malicious treatment of the device.

XX. Student Privacy

For the safety and privacy of the student, students may not post information in any form except directory information on the Internet without express parental permission.

Search and Seizure

Students have no right of privacy in materials sent, received or stored in District's Technology Resources. District officials may review system use at any time to determine if such use meets the criteria set forth in School Board policies and this AUP. Moreover, routine maintenance and monitoring of the District Technology Resources may lead to the discovery that a student has or is violating this Acceptable Use Policy, the Student Code of Conduct or other School Board Policies and regulations governing student discipline or the law. When an issue is discovered, an individual search will be conducted when there is a reasonable suspicion that the student has violated the law, the Student Code of Conduct or School Board Policies or regulations governing student discipline. The nature of the search/investigation will be reasonable and in accordance with the nature of the alleged misconduct.

Personal Devices and Network Security

To ensure the security of the Districts Technology Resources and to maintain a focused and equitable educational setting, students are prohibited from using personal electronic devices to connect to the district's networks. All students must use district-issued devices for all classroom activities during school hours. This policy helps protect from cybersecurity risks and ensures that all students have consistent access to the educational tools and resources provided by the district.

Disclaimer and Limitation of Liability

Pursuant to the Children's Internet Protection Act, Clint ISD uses filtering software to screen Internet sites for obscene material, child pornography, or any material that is harmful to minors. The Internet is a vast collection of worldwide networks and organizations that contain millions of pages of information. Students are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content, Nudity, Sex, Gambling, Violence, Weapons, Hacking, Racism, Hate, Tasteless, Illegal, and Questionable. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with

highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. No filtering software is one hundred percent effective, and it is possible that the software could fail. If the filtering software is unsuccessful, and children or staff gain access to inappropriate and/or harmful material, the District shall not be held liable. the District makes no warranties of any kind, either express or implied, that the functions of the services provided by or through the District's Technology Resources will be error-free or without defect. The District shall not be liable for Students' inappropriate use of the District's Technology Resources, violations of copyright restrictions, Students' mistakes or negligence, or costs incurred by Students. The District shall not be responsible for ensuring the availability of third-party District's Technology Resources or the accuracy, age appropriateness, or usability of any information found on electronic resources, including the Internet.

Consequences

If a student violates any of the provisions stipulated in this AUP, his or her privileges to the District's Technology Resources and data will be denied, and disciplinary action may be taken. The student in whose name a system account and/or computer hardware is issued will always be responsible for its appropriate use. Noncompliance with applicable regulations may result in suspension or termination of privileges and disciplinary action. 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. Disciplinary actions will be consistent with Board policy and the Student Code of Conduct tailored to meet the specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network.

THIS ACCEPTABLE USE POLICY DOCMENT IS FOR YOUR INFORMATION.
PLEASE USE IT TO HELP YOU FILL OUT
THE APPROPRIATE FIELD(S) IN THE OF THE ONLINE REGISTRATION MODULE.

THIS FORM DOES NOT NEED TO BE TURNED INTO THE CAMPUS

I understand and will abide by the Clint ISD 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.

PARENTAL PERMISSION/DENIAL OF PERMISSION FOR CHILD'S PARTICIPATION IN DISTRICT'S ELECTRONIC COMMUNICATION SYSTEM

I have read the District's electronic communication system policy CQ, Internet Safety Plan and administrative regulations available online at www.clintweb.net. In consideration for the privilege of my child using the District's electronic communication system, and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including, without limitations, the type of damage identified in the District's policy and administrative regulations.

I, the undersigned, in consideration of the Clint ISD or a contracted representative of the Clint ISD taking a photograph/video in a professional or like manner, do hereby voluntarily and knowingly execute this release with the express intention of relinquishing and giving all rights, titles and interest I may have in the finished picture, negative, reproductions and copies of the original prints, negative and videos and further give my permission that said finished pictures/videos of myself/legal guardian dependent may be used by the Clint Independent School District as they may deem proper for educational or informational purposes.