CLINT INDEPENDENT SCHOOL DISTRICT (03/2022)
TECHNOLOGY & INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY AGREEMENT

All individuals granted access to, or use of district technology and information resources must be aware of and agree to abide by the following acceptable use requirements:

Definitions	• **The District**: Clint Independent School District • **District Technology & Information Resources**: All computer and telecommunications equipment, software, data, and media, owned or controlled by district or maintained on its behalf. • **Information Security Office**: A division within the Technology Information and Services Department that oversees district cybersecurity. • **Information Security Officer**: The designated District Cybersecurity Coordinator per SB820 • **district data**: All data or information held on behalf of the district, created as result and/or in support of district business, or residing on District Information Resources, including paper records. • **Confidential data** or **Confidential Information**: All district data that is required to be maintained as private or confidential by applicable law. • **User**: Any individual granted access to district information resources.
General	• District Information Resource s are provided for the purpose of conducting district business however, Users are permitted to use District Information Resource s for use that is incidental to the User's official duties as permitted by this policy. • Users who are district employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the district have no expectation of privacy regarding any district data they create, send, receive, or store on district owned computers, servers, or other information resources owned by, or held on behalf, of the district. The district may access and monitor its information resources for any purpose consistent with district's duties and/or mission without notice. • Users have no expectation of privacy regarding any district data residing on personally owned devices, regardless of why the data was placed on the personal device. • All Users must comply with applicable district Technology Information Resources Use and Security policies at all times. District policy can be found online here: https://pol.tasb.org/Home/Index/436 • Users shall never use district Technology Information Resources to deprive access to individuals otherwise entitled to access district Information; to circumvent district computer security measures; or, in any way that is contrary to the district's mission(s) or applicable law. • Users must not interfere with the activities of others or use a disproportionate share of information resources. Examples of inappropriate use of resources are shown below. These actions frequently result in complaints and subsequent disciplinary action. ○ Sending an unsolicited message(s) to a large number of recipients (known as "spamming the network"). ○ Consuming an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications). ○ Deliberately causing any denial of service, including flooding, ICMP (Internet Control Message Protocol) attacks, or the unauthorized automated use of a service intended solely for human interaction. • Use of District Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited, unless such use is required as part of the User's official duties as an employee of the district and is approved in writing by the supervisor or a specific designee. Viewing, accessing, storage, and/or transmission of sexually explicit materials as incidental use is prohibited. • Users should report misuse of District Information Resource s or violations of this policy. How an incident is reported depends upon the nature of the incident: ○ If Users believe that their personal safety is threatened, they may call district security, 915-926-HELP (915) 926-4357 ○ For other incidents, Users should contact the Information Security Office or Department of Technology at tech_admin@clint.net. ○ For reporting problems with "spam" or unsolicited mail, Users should contact the Technology & Information Security Office at emailabuse@clint.net or tech_admin@clint.net .

Confidentiality & Security of data	• Users shall access district data only to conduct 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 district data in accordance with district's Records Retention Policy and Records Management Guidelines.
	• Users must not use or disclose confidential district data, or data that is otherwise confidential or restricted, without appropriate authorization. Examples of groups that can provide appropriate authorization include, but are not limited to Department of Business Services, Department of Human Resources, Department of Technology and Information Services, and the district's Public Information Officer.
	  ○ Users must ensure any individual with whom confidential district data is shared is authorized to receive the information.
	  ○ Users may not share district confidential data with friends or family members.
	  ○ Users may not share district business data that may be classified as confidential data, such as the status of negotiations, terms of contracts, and new research or products or relationships under development.
	  ○ Users will comply with the district's agreements to protect vendor information such as software code, proprietary methodologies, and contract pricing.
	• If User's office routinely receives requests for district confidential data, work with an appropriate group within the district to develop formal processes for documenting, reviewing, and responding to these requests.
	• If Users receive a non-routine request for district confidential data from a third party outside of the district, check with an appropriate group within the district to make sure the release of the data is permitted.
	• Users must report violations of district policies regarding use and/or disclosure of confidential or restricted information to the Information Security Office (tech_admin@clint.net, 915-926-4104).
	• Whenever feasible, Users shall store confidential information or other information essential to the mission of district on centrally managed services, rather than local hard drives or portable devices.
	• Confidential or essential district data stored on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smartphone, must be encrypted in accordance with district and any other applicable requirements.
	• All confidential district data must be encrypted during transmission over a network.
	• Users who store district data using commercial cloud services must use services provided or sanctioned by the district, rather than personally obtained cloud services.
	• Users must not try to circumvent login procedures on any District Information Resource or otherwise attempt to gain access where they are not allowed. Users may not deliberately scan or probe any District Information Resource without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences.
	• All computers connecting to a district's network must run security software prescribed by the Information Security Officer as necessary to properly secure District Information Resources.
	• Devices determined by district to lack required security software or to otherwise pose a threat to District Information Resources may be immediately disconnected by the district from a district network without notice.

Email	• Emails sent or received by Users while conducting district business are district data that are subject to state records retention and security requirements.
	• Users are to use district provided email accounts, rather than personal email accounts, for conducting district business.
	• The following email activities are prohibited when using a district provided email account:
	  ○ Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose (delegated access).
	  ○ Accessing the content of another User's email account except 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of district.
	  ○ Sending or forwarding any email that is suspected by the User to contain computer viruses.
	  ○ Any Incidental Use prohibited by this policy.
	  ○ Any use prohibited by applicable district policy.

Incidental Use of Information Resources	• Incidental Use of District Information Resources must not interfere with User's performance of official district business, result in direct costs to the district, expose the district to unnecessary risks, or violate applicable laws or other district policy. • Users must understand that they have no expectation of privacy in any personal information stored by a User on a District Technology Information Resource, including district email accounts. • A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located. • Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited. • Users may not be paid, or otherwise profit, from the use of any district-provided information resource or from any output produced using it. Users may not promote any commercial activity using District Information Resources. Any such promotions are considered unsolicited commercial spam and may be illegal as well. • Incidental use for purposes of political lobbying or campaigning is prohibited. • Storage of any email messages, voice messages, files, or documents created as Incidental use by a User must be nominal.
Additional Requirements for Portable and Remote Computing	• All electronic devices including personal computers, smartphones or other devices used to access, create, or store District Information Resources, including email, must be password protected in accordance with district requirements, and passwords must be changed whenever there is suspicion that the password has been compromised. • District data created or stored on a User's personal computers, smartphones, or other devices, or in data bases that are not part of District's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to District Information Resources. • District issued mobile computing devices must be encrypted. • Any personally owned computing devices on which Confidential district data is stored or created must be encrypted. • User agrees for the district to enforce mobile device management on any personally owned devices in case the device is lost or stolen. • District data created and/or stored on personal computers, other devices and/or non-district databases should be transferred to District Information Resources as soon as feasible and removed from personal devices. • Unattended portable computers, smartphones and other computing devices must be physically secured. • All remote access to networks owned or managed by district must be accomplished using a remote access method approved by the district, as applicable.
Password Management	• District issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone. • Users must not give others access to District Information Resources unless they are authorized and authenticated for such access. Users may not extend access to District Information Resources to others without permission (e.g., proxy services, accounts for non-district personnel, etc.). • Each User will be held responsible for all activities conducted using the User's password or other credentials.

User Acknowledgment (*or via electronic signature*)

I acknowledge that I have received and read the Technology & Information Resources Acceptable Use Policy. I understand and agree that my use of District Technology Information Resources is conditioned upon my agreement to comply with the Policy and that my failure to comply with this Policy may result in disciplinary action up to and including termination of my employment.

Signature: Date:

Printed Name: