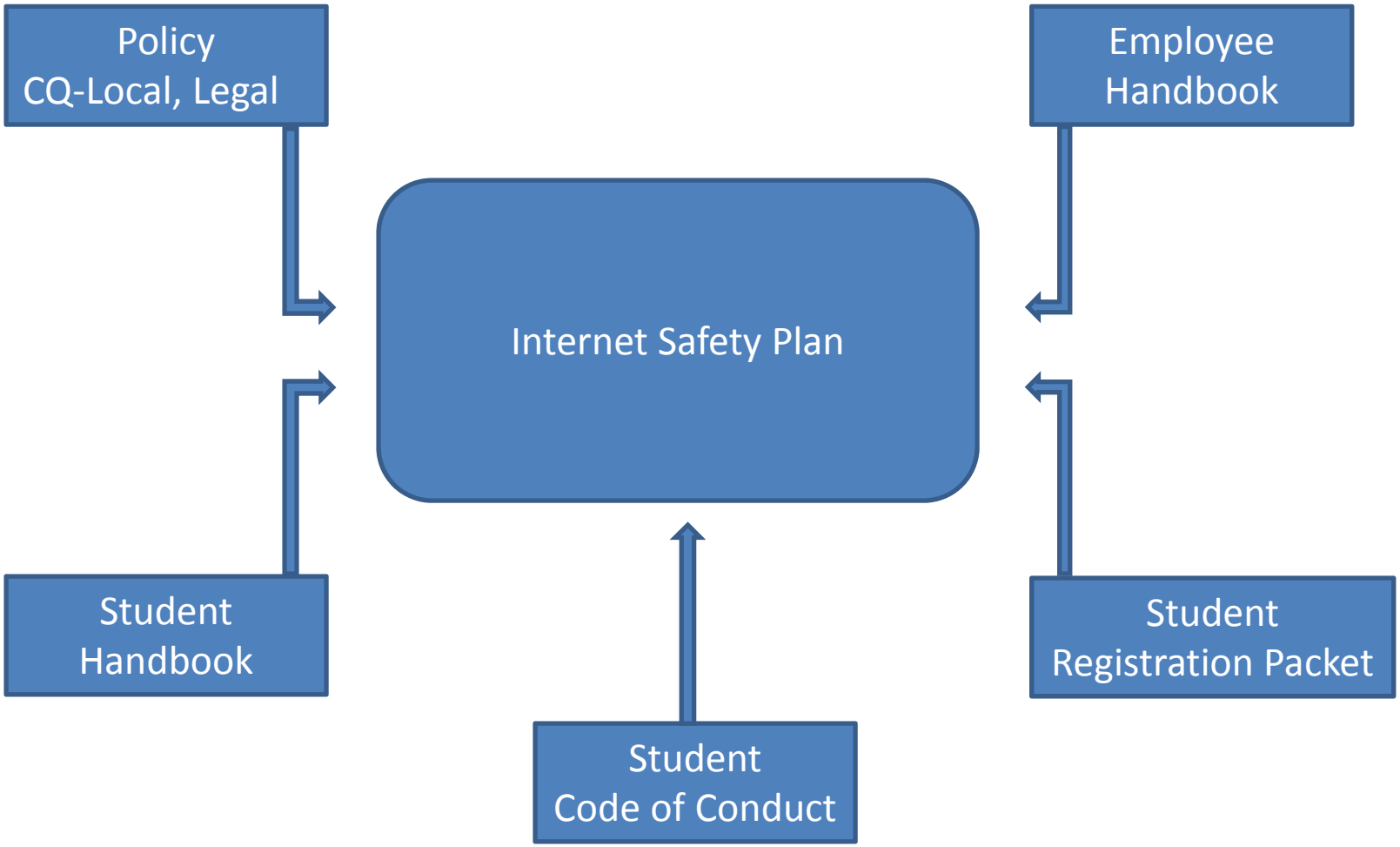
Clint ISD
Internet Safety Plan
Linked Components



Updated 05-30-2012

Clint Independent School District

Internet Safety Plan

The district's Internet safety plan and procedures are required by board policy CQ (Legal and Local), including compliance in supporting the federal requirements of the Children's Internet Protection Act (CIPA) and the Protecting Children in the 21st Century Act.

This document serves as the first step towards ***acknowledging*** acceptable use, ***consequences***, and ***awareness*** of Internet resources. This includes ***educating*** our students and employees on the proper responsible use of these resources (safety on the Internet, appropriate behavior and cyberbullying awareness and response).

This document ties together related information described in supporting district policy CQ legal and local, the Student Code of Conduct, Student Handbook, Student Registration Packet, and the Employee Handbook, available online at www.clintweb.net. This document will be reviewed annually and changed as necessary to comply with all district policies, including federal and state laws.

The Clint Independent School district's Internet safety plan's purpose is to ***prevent and protect*** students and employees by ***identifying, educating, monitoring***, ***documenting*** and ***reporting*** the use of safe practices (cybersafety) and policies when utilizing the Internet and its related resources/topics within Clint ISD.

These areas include, but are not limited to:

• Acceptable and unacceptable use	• Email	• Monitor and content filtering	• Spam email
• Blogging or Tweeting	• File sharing	• Predators online	• Tweeting
• Chat rooms	• Gaming	• Program downloading	• Web cams
• Cell phones	• Identify theft	• Proxy access	• World Wide Web (www)
• Copyright and plagiarism	• Hacking	• Sexting	• Video streaming
• Cyberbullying	• Inappropriate content	• Social networking	• Virus protection

(see Section 5. Glossary)

Section 1. Acknowledging acceptable use, ***consequences*** and ***awareness*** of Internet resources.

Access to the Clint ISD network, the Internet, or other computer networks through the use of computer equipment, mobile devices or network connections, wired or wireless, sponsored by the Clint Independent School District shall be regulated and governed by the Board of Trustees, the Superintendent, and/or their designees. This includes district provided cell phones, telephones and email communication access. The district provides access to networks for the purpose of supporting instructional programs, expanding educational opportunities, promoting academic growth, and improving the overall organizational efficiency of the district. However, the district recognizes that not only can computer technology enhance the educational experience for students, but it can also lead to inappropriate, disruptive, and illegal actions that must be monitored and regulated by the district. Prudent implementation of computer networks and related technologies in our schools requires that we strive to provide computer environments that are

(1) Safe for students to use.
(2) Productive for teachers and district employees.
(3) Guided by ethical conduct and community standards.
(4) To prevent the use or access of resources over its computer network to, or transmission of inappropriate materials that are harmful to students and minors via the Internet, World Wide Web, electronic mail, chat rooms, and/or other forms of direct electronic communications.
(5) To prevent unauthorized access, including hacking, and
(6) To educate students about cyber-bullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking web sites and chat rooms 47 U.S.C. 25 (h (5)(B)(ii). Therefore, the following guidelines for acceptable computer use are provided to all students and employees of the district: Definition: "Harmful to students and minors" means any picture, image, graphic image file, or other visual depiction that:

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

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for students and 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

3. Taken as a whole lacks serious literary, artistic, political, or scientific value as to students and minors, 47U.S.C. 254(H)(7)(G):20U.S.C.6777(e)(6)

The district provides use of computer, mobile devices and computer networks, wired or wireless, that promote:

- Education, academic growth, scholarship, and citizenship
- Educational research and professional growth
- Efficient organizational communication and professional collaboration
- Community improvement, economic development, and public service
- Democratic principles, liberty, and social responsibility

The district deems as unacceptable and prohibits use of computers, mobile devices, applications or programs and computer networks, wired or wireless, that promote:

- Any violation of United States or state laws, including copyright infringement.
- Willful disruption of network services or interference with normal computer operations including attempting to disable any Internet filtering device, computer security measures, unauthorized use of Internet proxy programs or other programs designed to gain unauthorized access.
- Willful introduction of propagation of computer viruses, worms, or damaging malicious or unauthorized programs.
- Assuming a false network identity or using an identity other than one's own.
- Plagiarism, misrepresentation of digital resources, or theft of intellectual property.

• Transmission or receiving of obscene, pornographic, or sexually explicit messages, or other inappropriate materials through any electronic means such as email, blogs, proxies, list serves or postings of non-sponsored web sites.
• Use of network services or applications for profit, personal gain, commercial purposes or political lobbying.
• Anti-social behavior by posting messages that are damaging to another's reputation, overtly annoying, harassing or demeaning through any electronic means such as email, blogs, texting, tweet, list serves, videos, or postings on web sites or social networks not authorized by Clint ISD.

The Clint Independent School District will increase connectivity to global networks and expand technologically based opportunities for students as much as possible. It is, however, also the responsibility of the district to limit, filter and control access to inappropriate network content through whatever means the district can reasonably provide.

Full access to the Internet can provide students with many instructional resources and educational opportunities, but it can also provide them with access to content that is confusing, demoralizing, and damaging. It is the responsibility of the district to safeguard what is in the best interest of students, a teacher, employees and the communities as technological decisions regarding network content are made. Use of computer networks, wired or wireless, cannot be completely monitored or controlled – it is virtually impossible. Therefore, it should be understood that any user of a CISD sponsored network or network application, wired or wireless, bears a personal responsibility to use computer networks in ways that are ethically, morally, and legally consistent with the purpose of the district to promote a healthy environment and opportunities for student success. In addition, if any individual observes or witness any inappropriate use of computers, mobile devices, computer applications, computer networks, or any technology resources; it is their responsibility to report this violation to any campus teacher, principal or district administrator as soon as possible. Failure to report such an incident may result in disciplinary or legal action in accordance with the Student Code of Conduct, Employee handbook, district policies and applicable laws.

Section 2. Prevent and protect students and employees by i***dentifying and educating*** the use of safe practices (cybersafety)

Protecting students and employee safety is Clint ISD's priority when accessing the Internet or related resources. Clint ISD has installed protection measures district-wide that include the following:

Firewalls – protects the boundary of the internal Clint ISD network from the public Internet. They also aid in preventing unauthorized access to application system data including student and employee information.

Internet content filtering – a subscription based category filtering system that blocks inappropriate content areas of the Internet that are harmful to minors, contain visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA) and included in district policy CQ (Legal and Local). If a web site has been determined to be miscategorized, a teacher, administrator or employee can request access to the site by contacting their supervisor and filing a SchoolDude Ticket request form. The site's content will be reviewed by the Technology and Information Services department for its educational usefulness and modified as required. The district utilizes Internet content filtering programs and appliances as the protection measure in place for all Internet enabled computers or mobile devices used by students or staff. As per district policy CQ (Legal and Local), the district may disable the filtering device for bona fide research or other lawful purpose.

Cybersafety – Educating students on appropriate online behavior, including interacting with other individuals on social networking websites, texting and chatting including cyberbullying awareness and response is accomplished through an online student cyber safety course. The cyber safety course is facilitated by the Instructional Technology Services department. Student email is provided to all students in grades 2 through 12. Access to the email system must first be accomplished by passing the online cybersafety course. The course consists of a series of cyber safety videos covering topics that range from social media interactions, electronic communications (chatting/texting), content postings, protecting personal identifying information, virus protection, and cyberbullying awareness and prevention. Following the video, the student is required to pass a quiz and accept a cybersafety pledge. Once completed, the student receives a cybersafety certification of completion.

To further promote Cybersafety, Clint ISD participates in the El Paso Regional Cyber Safety Cooperative. The cooperative is a combined effort of school districts and the Texas educational service center in the Region 19 area to identify and promote Cybersafety. Information on Cybersafety tools and resources including ethical Internet behavior for children is available to parents and all school personnel. The site is actively available on the district's web site but can be directly accessed at http://www.esc19.net/eprcsc.

Student email system – Clint ISD uses Microsoft Office 365 a subscription based email system for students in grades 2 through 12 and all district employees which contains filtering components which:

- Blocks inappropriate words, domains, addresses and attachments
- Provides Anti-Spam measures
- Students must complete a Cybersafety course to access email
- Email message safety rules based on "keywords" that identify questionable messages and reports information to authorized district administrators for review and action.

Learning Management system – Clint ISD uses the Google Suite for Education for student and teacher use for communication and collaboration. All administrative actions for student and teacher accounts are administered from a single dashboard. This includes identifying and providing a Google Account and granting access to Google Apps and resources.

Anti-Spam system – A subscription based category filtering system that prevents and blocks spam, junk and scam email from entering the district's email system. This includes aiding in reducing exposure to potential identify theft emails and programs. These protection measures are part of the district's virus protection program.

Virus protection – all computers in Clint ISD are installed with antivirus and antispyware protection programs. These programs help to protect, block, remove and repair virus attacks such as Trojan horses, worms, malicious Internet bots, blended threats, hacking tools, remote access programs, spyware and trackware, including helping to protect access to personally identifiable information. Scheduled subscription updates and scanning aid in the detection, quarantine and removal process.

Workstation lockdown – software based policies are used to lockdown administrative access control for computer workstations. This aids in preventing hacking and unauthorized access to programs. Many computer labs and computers on wheels (COWs) contain these software programs.

Application Passwords – Access to student and employee information is also secured by authorized users with password access using Active Directory. Users are required to change their application system passwords a minimum of every 200 days. Regularly changing application passwords helps to minimize unauthorized access to account information or personnel data.

Network Etiquette – Educating all students and staff on the proper use of Internet and related computer application and electronic communication systems is vital in ensuring the most effective use of these resources and in becoming ethical 21st century learners. Online cyber safety courses such as the ones provided through the district's training initiative to provide essential resources. In addition, classroom monitoring, content filtering and teaching by example further help to promote safe travel through the World Wide Web. Network Etiquette is simply abiding and following the rules as described in section 1.

Section 3. Monitoring, Documenting and Reporting

Monitoring and **Reporting** – allows the district to measure, report, and verify the following areas:

- Determine Internet content filtering subscription updates are taking place.
- Determine Internet content filtering is correctly blocking inappropriate content either directly or indirectly by each district Internet enabled device such as computers or mobile devices.
- Identify Internet sites that are most active or used including categories and locations.
- Measure current Internet bandwidth and help to project future needs
- Determine virus protection measures are actively running and scheduled updates are taking place.
- Report on students completing cyber safety coursework.
- Classroom monitoring, observations and supervision by teachers and staff on proper online behavior.
- Bullying prevention hotline telephone numbers are available at each campus and routed to the associated campus counselors office. Web site announcement for bullying prevention are also available on the district web site.
- Report on Internet or network incidents. Internet / Network Incident forms are used when reporting and investigating policy violations.

Documenting – allows the district to document policies, proper responsible acceptable use, consequences and procedures relating to the use of technology resources and electronic communications. These areas include but are not limited to:

- Federal and State requirements and laws are being addressed and followed.
- District policies and regulations updated and in place.
    - CQ (Local and Legal) – Technology Resources
    - BBI (Local) – Board Members – Technology Resources and Electronic Communications
    - CPAC – Office Communications Telephone
    - CY (Local and Legal) - Intellectual Property
    - DH (Local and Legal) – Employee Standards of Conduct
    - FL (Local and Legal) – Student Records
    - FNC (Local and Legal) – Student Rights and Responsibilities – Student Conduct
    - FNCE (Local and Legal) – Student Conduct – Personal Telecommunication/Electronic Devices
    - GBAA (Local and Legal) – Information Access – Requests for Information
- Internet Safety Plan updated and in place.
- Student handbook, Code of Conduct and registration packets are updated and in place. Student and Parent signatures are on file representing acceptance of responsible use.
- Employee handbook is updated and in place. Employee signatures are on file representing acceptance of responsible use.
- Individual employee access to business and student systems are requested through the district's security request form process. Request for access is available internally through the district's web site under the Employee tab. Requests are routed for review and approval before final acceptance.
- Special Security Access request forms are available internally through the district's web site under the department of Technology and Information Services. Requests are reviewed for approval before final acceptance.

Section 4. Compliance

The district's Internet Safety Plan must address the following CIPA requirements

1. Controlling students' access to inappropriate materials, as well as materials that are harmful to minors.

   Addressed: YES

   Section 1. Acknowledging acceptable use, consequences and awareness of Internet resources
   Section 2. Prevent and protect
   Section 3. Monitoring, Documenting and Reporting

2. Ensure student safety and security when using electronic communications.

   Addressed: YES

   Section 1. Acknowledging acceptable use, consequences and awareness of Internet resources
   Section 2. Prevent and protect
   Section 3. Monitoring, Documenting and Reporting

3. Prevent unauthorized access, including hacking and other unlawful activities.

   Addressed: YES

   Section 1. Acknowledging acceptable use, consequences and awareness of Internet resources
   Section 2. Prevent and protect
   Section 3. Monitoring, Documenting and Reporting

4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

   Addressed: YES

   Section 1. Acknowledging acceptable use, consequences and awareness of Internet resources
   Section 2. Prevent and protect
   Section 3. Monitoring, Documenting and Reporting

5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms

   Addressed: YES

   Section 1. Acknowledging acceptable use, consequences and awareness of Internet resources
   Section 2. Prevent and protect
   Section 3. Monitoring, Documenting and Reporting

Accepted policies through public hearing for CIPA Compliance on: April 17, 2012

Section 5. Glossary of Terms

The terms below are provided to describe a brief explanation of their definition. Further detailed information can be obtained by searching the web through a search engine such as Google, Yahoo, Bing and many others.

Acceptable and unacceptable use: Defines the acceptable and unacceptable uses of Internet resources and electronic communication devices by students and employees of Clint ISD. *See Inappropriate content*

Blog or Blogging: Comments or discussion messages usually on any specific topic posted on a blogging site on the Internet. A person who blogs is considered a blogger.

Chat rooms: Where users communicate to each other with simple short messages, similar to texting but located on an Internet site.

Cell phones: or mobile phones are wireless telephones with subscription pricing plans from telephone carriers. Some phones have data capabilities to text, access the Internet and take pictures, typically called "smart phones"

Copyright: Typically an owner's exclusive legal right to prohibit other individuals from using their works such as written papers, books, music, artwork or other material without the owner's permission.

Cyberbullying: Refers to bulling through communication devices such or cell phones, computers or Internet resources. These include blogging, texting, chat rooms, instant messages, social networking web and other web sites.

Email: Electronic mail where mail messages are exchanged between people digitally over private networks and the public Internet.

File Sharing: Process of sharing electronic files between users. These files can be documents, music, audio, videos or other digital files. The files are usually stored on a computer network server and shared between users.

Gaming: Electronic games or programs that people play on devices ranging from home gaming centers to cell phones and computers. Some allow you play against other people over communication networks like the Internet.

Identify theft: A form of stealing one's personal information or identity in order to use for achieving some form of monetary gain, such as falsely using one's credit cards, bank information or social security number.

Hacking: Individuals or groups that attain unauthorized access into electronic computer applications or communication network resources. Typically this is accomplished by breaking into such systems, locally or remote, to possibly gain access for information, change or damage to the system. A person who hacks is considered a hacker.

Inappropriate content: Content or information that is determined to be inappropriate or harmful to minors. Categories include visual depictions that are deemed obscene, child pornography, violence, illegal activities, and others areas that are considered unsuitable for a student's educational use. *See Acceptable and unacceptable use*

Monitor and content filtering: The process of monitoring the effectiveness and updates of Internet content filtering. Content filtering removes or restricts inappropriate content from the Internet to an electronic device.

Plagiarism: Considered a form of cheating when using someone else's words or ideas and falsely representing it as their own.

Predators online: People who use online communication resources like Internet chat rooms, instant messaging or social networking sites to sexually target and befriend children. They build a false sense of friendship for some form of sexual satisfaction or other unlawful activities.

Program downloading: Computer program or online resource that allows for downloading programs or files. See File Sharing

Proxy access: Using computer resources to anonymously access programs, information and network resources like the Internet. A proxy server makes requests for information on behalf of an anonymous user by hiding the requesting user's identity.

Sexting: The process of sending and sharing sexually explicit messages, photos or videos over cell phones.

Social networking: An online service that caters in emphasizing individuals to form groups to share ideas and information including meeting other or like people with similar interests or experiences. Internet places such as Facebook or Myspace are considered social networking sites.

Spam email: Unwanted or unsolicited email messages considered to be junk mail usually sent in bulk to many individuals at the same time. Anti-Spam filtering programs and services help to filter and remove unwanted spam email.

Tweeting: A short text posting or instant message on a social networking site like Twitter. Tweeting is also considered micro-blogging.

Web cams: A computer video camera that when connected to a computer or network can capture real time video and transfer it across networks like the Internet. These images can be captured and saved to network server Internet sites like YouTube and played when convenient or displayed in real time like a Ustream broadcasting site. *See Video streaming*

World Wide Web (www): Also referred to as the Internet. The global communications network that allows anyone to browse, post or share digital information when connected. The Internet can be accessed through computers, cell phones, mobile devices and other Internet enabled devices.

Video streaming: The process of sending video or multimedia content over computer networks like the Internet to viewers in real time. *See Web cams*

Virus protection: A computer program or set of programs used to protect against computer viruses or other malicious code attacks to a computer workstation, computing device or communication network.