Technology Resources
LISD Acceptable Use Policy

Administrative Regulation CQ

INTRODUCTION

Lovejoy ISD incorporates technology as a natural part of the educational process. The use of educational technology empowers students and fosters the development of life-long learning skills through access to the latest equipment, information, and resources. Computers and technology are integrated into every facet of the educational and administrative process. Lovejoy ISD endeavors to provide appropriate educational technology and the skills required to use this technology responsibly for all students in order to prepare them for the classroom and workplace of tomorrow.

Lovejoy ISD's educational technology includes campus-wide and District-wide computer networks utilizing direct Internet access. Distance learning, streaming web-based video content, electronic mail and fax services are also available. Secure access firewalls and content-filtering software are utilized in order to protect students from inappropriate content on the Internet/World-Wide Web.

The Lovejoy ISD Acceptable Use Policy explains and defines the responsible and ethical use of educational technology for all students and staff. All rules embodied herein guide students in appropriate and acceptable use of District technology, and are designed to protect both the student and the District.

Access to technology and electronic communication systems, including computer networks and the Internet, is made available exclusively for instructional purposes in accordance with District guidelines and regulations. Access to these systems is a privilege, not a right.

The Lovejoy ISD Acceptable Use Policy applies to all users of Lovejoy ISD's Electronic Communications Systems. Users include:

- Lovejoy ISD employees
- Lovejoy ISD students
- Contractors
- Consultants
- Student Teachers
- Temporary workers
- Any third parties that use the system

BOARD POLICY [CQ (LOCAL)]

DATE ISSUED: 5/17/2011
UPDATE 90
CQ(LOCAL)-A

TECHNOLOGY RESOURCES

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

For purposes of this policy, “technology resources” means electronic communication systems and electronic equipment.

Access to the District’s technology resources, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations.

Limited personal use of the District’s technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District’s technology resources; and
3. Has no adverse effect on an employee’s job performance or on a student’s academic performance.

Access to the District’s technology resources, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District’s technology resources.

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

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 the 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.

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
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.

Each District computer with Internet access and the District's network systems shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or another authorized person may disable the filtering device for bona fide research or other lawful purposes.

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.

The District shall not be liable for users' inappropriate use of the District's technology resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.

A District employee shall retain electronic records, whether created or maintained using the District's technology resources or using personal technology resources, in accordance with the District's record management program. [See CPC]

Upon discovering or receiving notification of a breach of system security, the District shall disclose the breach to affected persons or entities in accordance with the time frames established by law.

The District shall give notice by using one or more of the following methods:
1. Written notice.
2. Electronic mail, if the District has electronic mail addresses for the affected persons.
3. Conspicuous posting on the District's website.
4. Publication through broadcast media.

Lovejoy ISD Acceptable Use Policy

Definitions

Electronic communications include any use of electronic communications equipment or LISD system. The electronic communications system includes:

- Computers/Laptops
- Handheld devices
- Lovejoy ISD's internal network (including the wireless network)
- The Internet
- Lovejoy ISD's telecommunications system including telephones
- Lovejoy ISD's voicemail system
- Lovejoy ISD's email system
- Lovejoy ISD's printers
- Lovejoy ISD's fax machines
- Lovejoy ISD's remote access services (VPN)
- Any other electronic communications equipment used on LISD property
- Any third-party equipment used on Lovejoy ISD's electronic communications system (including personally owned computers and individual's PDAs when connected to or used on Lovejoy ISD campuses).

For the purposes of this document, electronic communications system will be shortened to "system".

Any electronic device falls under the authority of the Lovejoy ISD Acceptable Use Policy if used on LISD property regardless of whether they may or may not be wirelessly connected to the District network infrastructure. For example, texting or emailing inappropriate pictures to other users while on district property would be a violation of the Acceptable Use Policy even if only done using the user's personal cellular plan and using no District provided network services.

Access

The Superintendent or designee will oversee Lovejoy ISD's system. Access to the system is a privilege, not a right:

- The immediate supervisor of the Lovejoy ISD employee must give approval for the Lovejoy ISD employee to have access to Lovejoy ISD's system. If the user is a third-party user, the user must submit to a request to the director of their department and the director of the department must give approval for the third-party individual to access Lovejoy ISD's system.
- Lovejoy ISD recommends that users change their system password on a regularly scheduled basis.
  Passwords are not to be shared with anyone.
- After school hours, Lovejoy ISD students have first priority for using Lovejoy ISD's system.

- Any user that is identified as a security risk by a system administrator may be denied access to Lovejoy ISD's system.
- Any user that has violated Lovejoy ISD and/or campus computer-use guidelines may be denied access to Lovejoy ISD's system.
- All Lovejoy ISD systems are monitored.
- The system will be used for administrative and educational purposes consistent with the district's mission and goals. Commercial, for-profit use of the system is strictly prohibited (see Employee Handbook - Use of School Equipment). Limited personal use of Lovejoy ISD's system is permitted.

Wireless Network

The district's wireless (WiFi) network is made available for general public use. Unlike free public WiFi hotspots similar to those provided at a Starbucks or McDonald's, the district's wireless network is filtered for acceptable content as described in the Internet Safety section below.

In accordance with the Student Code of Conduct, students in high school, with teacher permission, may use personal laptop and internet-enabled handheld devices on the wireless network of Lovejoy ISD for academic and instructional purposes. Students must meet the expectations stated below to protect the district network, as well as their personally owned devices. Use of devices for voice or text messaging must abide by district and campus policy.

Wireless internet-enabled devices may be used in public areas around campus where wireless services are provided. Students must login to the LISD network when using technology on campus. Students who are creating a disruption will be asked to put the device away. Students must ask permission of each individual teacher to use the device during an academic class.

Expectations:

- The student must have a signed AUP and follow all conditions and acceptable use of the network as outlined in the district's Acceptable Use Policy.
- The owner of the device is solely responsible for the physical security and the network security of the device, even when shared/loaned to another student.
- The owner is solely responsible and capable of setting up the device on the wireless network and provides all necessary equipment such as the battery, power supply, and connections.
- Student-owned devices MUST ALWAYS be connected to the school's wireless network to access the internet.
- With permission of a teacher, students may charge their device in an academic room.
- School staff will NOT provide technical support for personally owned devices.

Training

Lovejoy ISD will provide training to users in proper use of the system and will provide all users with copies of the Lovejoy ISD Acceptable Use Policy. All Lovejoy ISD training for the system will emphasize its ethical use.

Copyrighted Materials

Copyrighted software of data may not be installed on the system without permission from the holder of the copyright. Only the owner of the copyright (or individuals the owner specifically authorizes in writing) may upload copyrighted material to the system.

Posting Practices

Assisted by district staff, designated campus personnel will maintain the campus web pages. The district provides web space for departments and professional personnel through a district-approved application.

The use of student names, pictures, and/or student-generated work on Lovejoy ISD's public network, web pages or other approved online sites, is considered acceptable unless the parent or guardian objects to this use.

- All departments and professional staff must use the district's approved applications for their district web pages and online content.
- District and campus web pages may contain individual pictures, group pictures, first names, and/or when appropriate last names of students.
- Parents or guardians may object to this use as part of the Student Code of Conduct, Student Handbook, Technology Acceptable Use, and FERPA acknowledgment process.

Internet Safety

Lovejoy ISD will use technology protection measures to prevent users and students from accessing inappropriate material deemed harmful to minors. Technology Protection Measures are defined as specific technologies that block or filter Internet access to inappropriate content. These protection measures are used on both wired and wireless devices that access the district's system. Inappropriate content is defined as:

- Obscene, as defined in section 1460 of title 18, United States Code.
- Child pornography, as defined in section 2256 of title 18, United States Code.
- Harmful to minors (including websites about violence, racism/hate).
- Disruptive to learning in the classroom (including sites with non-educational games).
- Inappropriate for minors (including websites that contain hacking instructions, Adware, Spyware, and SPAM Internet fraud and scams).

- Harmful to the technology protection measure (including websites with proxy servers that can be used to bypass the filters).
- Illegal (including piracy websites).

While LISD will make every effort to prevent it, we cannot guarantee that users may not gain access to inappropriate material. There may be additional kinds of material on the Internet that are not in accord with your family values. Lovejoy ISD would encourage you to use this as an opportunity to have a discussion with your child about family values and your expectations about how these values should guide your child's activities while they are on the Internet.

Controls on the technology protection measures may be updated daily. Sometimes the controls may prevent access to sites needed for educational or administrative use. If a user needs to access a blocked site, they may submit a request to have the Website reviewed.

- Users will behave in an ethical and legal manner when they use the Internet. They realize that they are entering a global community and their actions reflect on Lovejoy ISD as a whole
- Students may not give out their address, telephone numbers, passwords credit card information, or any other personal information on the Internet without express written parental permission

Responsibilities

The Superintendent will designate a district-level coordinator to

- Disseminate and enforce acceptable use policies and guidelines at the district level.
- Ensure that all users read and sign an agreement to abide by Lovejoy ISD's policies and guidelines regarding the use of the system. The central office will file and store the agreements signed by users. Campus personnel will store student signed agreements.
- Monitor activity on the system (as needed).
- Establish a retention schedule for messages on any electronic bulletin board.
- Remove local messages that are inappropriate.
- Set limits for disk utilization.

Principals will designate campus-level coordinators to

- Disseminate and enforce acceptable use policies and guidelines at the campus level.
- Ensure that teachers adequately supervise their students and are responsible for their students' use of the system.
- Ensure that teachers who supervise students provide training to students that emphasize appropriate use of the system.

Individual Users

Are responsible for their system account and will use the account properly. Users take full responsibility for their action and will use the Lovejoy ISD system and the Internet for educational purposes. Users:

- May not use Lovejoy ISD's system for illegal purposes, in support of illegal activities, or for any other activity prohibited by Lovejoy ISD policy.
- May not use another user's system account without written permission from the Lovejoy ISD coordinator. Students may not use another user's system account.
- Must keep their passwords protected. Users may not share their password with another person for any reason. Users may not write their passwords down and tape them to their monitor, tape them underneath their keyboard, or keep them anywhere where another person can see their password.
- Must keep personal use of their email accounts and phones to a minimum. Limited individual messages are acceptable.
- Must not let personal use of email interfere with their jobs.
- Must properly maintain their email accounts.
- Delete email in accordance with established email retention guidelines
- May only re-distribute copyrighted programs or data only with written permission of the copyright holder or designee. This includes downloading and opening executable files received as an email attachment.
- Must comply with the acceptable use guidelines and policies of any third-party systems that they access.
- Users must use the wireless network provided by the district and may not use personal wireless Network devices.
- Users must not download any software without prior approval from Lovejoy ISD's system manager or designee. The user is responsible for any costs incurred by downloading software.
- Users may not access, attempt to access, download, transmit, store, view, or bring to school any inappropriate content at any time.
- Must report any misuse of the system to the system administrator or appropriate supervisor.
- Users must not delete, copy or modify system files.
- Users may not transfer inappropriate or illegal materials through the Lovejoy ISD Computer system and/or Internet connection.
- Must back up their own data. Lovejoy ISD's system administrator recommends backing up essential data in three locations:
  - On your local computer's hard drive
  - On a network drive (your home directory, Google Drive, or a common drive).
  - On removable media storage (USB Flash drive).

Elementary students have access to district-approved apps on school-owned devices. Lovejoy always uses digital tools and apps in a way that is consistent with the

Children's Online Privacy Protection Act. Parents may deny access to any specific digital tool by notifying their child's campus administrator in writing.

Cyber-Bullying and Harassment

Threatening, harassing, and/or bullying others using electronic means to include the Internet and/or mobile technology is strictly prohibited. Students may not:

- Use the district's network for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, sex, gender, sexual orientation or disability.
- Send abusive text messages to cell phones, computers, or any electronic device.
- Post abusive comments on someone's blog or social network site.
- Create a social networking account or webpage that masquerades as the victim's personal site.
- Create a social networking account or webpage that masquerades as a district account.
- Post another individual's personal information.
- Send abusive comments.
- Record or distribute media with the intent to manipulate or embarrass others.

Vandalism and Abuse

Vandalism is an activity that intends to harm or destroy any part of the system, another user's data, or any agencies or network connected to the internet or using any means to possess vandalism tools on network drives, pen drives, removable media, or the local computer. Vandalism includes deliberate attempts to degrade or disrupt system performance. Vandalism includes, but is not limited to,

- Denials of Service (DOS) attacks
- Distributed Denial of Service (DDoS) attacks
- Uploading or creating viruses
- Using keystroke recording systems
- Loading Spyware or Adware
- Using port scanners or other tools to do network reconnaissance
- IP spoofing
- Man-in-the-Middle attacks
- Traffic sniffing
- Using any other tools to hack into or spy on the system

Vandalism is strictly prohibited and vandals will lose access to the system and must provide restitution for hardware and software costs associated with system restoration. Vandals may be prosecuted under applicable state and federal laws. Lovejoy ISD will cooperate fully with local, state, or federal officials in any investigation concerning or relating to vandalism of Lovejoy ISD's system or any other system.

Email Abuse

Attempts to read, delete, copy, or modify the electronic mail of other users or deliberate interference with the ability of other system users to send/receive email is prohibited. Forgery or attempted forgery of email is prohibited.

Plagiarism

Copying any content from the internet or the system that doesn't belong to the user and claiming that the content is the property of the user is prohibited. Users must cite the source when including from the Internet or the system.

Third-Party Content

Users and parents of students with access to the system should be aware that users and students might access other systems in the global network that may contain inaccurate and/or objectionable material. Any student or employee who brings prohibited materials into the system is subject to suspension, revocation of access, and is subject to disciplinary action in accordance with the Student Code of Conduct.

Revocation of Access

If any user violates the Acceptable Use Policy, Lovejoy ISD may suspend the user's access to the system. Lovejoy ISD will terminate the user's accounts on the date the principal or Lovejoy ISD coordinator receives notice of student withdrawal or revocation of system privileges, or on a future date if specified in the notice.

Disclaimers

System Access: Access to the system is provided on an "as is, available" basis. Lovejoy ISD does not make any warranties with respect to any services provided by the system and about any information or software contained on the system. Lovejoy ISD does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

User Information: Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system belong to the providers and not Lovejoy ISD.

Liability: Lovejoy ISD is not liable for inappropriate use of Lovejoy ISD's system or violations of copyright restrictions, mistakes or negligence caused directly or indirectly

by users, or costs that users incur. Lovejoy ISD is not responsible for ensuring the accuracy or usability of any information on the Internet.

Acknowledgment

I acknowledge that it is my responsibility to read, review and understand and comply with the Lovejoy ISD Technology Acceptable Use Policy. I understand that non-compliance with this policy may result in suspension of my access or termination of my privileges and other disciplinary action consistent with Board policies and state law.
[See the Student Code of Conduct, and Board Policies DH, FN series, and FO series.]

I realize that any of my actions that are violations of law may result in criminal prosecution as well as disciplinary action by the District. Any violation of this policy that results in system disruption or damage may result in the assignment of financial liability to me.

LOVEJOY INDEPENDENT SCHOOL DISTRICT
Internet Safety Policy

INTRODUCTION

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries.

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene, (b) child pornography, or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors. An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purposes.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

COMPLIANCE WITH THE REQUIREMENTS OF THE CHILDREN'S INTERNET PROTECION ACT

It is the policy of the Lovejoy Independent School District (LISD) to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA"). It is the goal of this policy not only to prevent and protect, but to educate employees, students, parents and the community of LISD in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by LISD into its Technology Acceptable Use Policy.

TECHNOLOGY PROTECTION MEASURES

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. LISD utilizes a sophisticated content filtering system on all computers that access the Internet, which is compliant with CIPA.

ACCESS TO INAPPROPRIATE MATERIAL

To the extent practical, Technology Protection Measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, as well as access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to administrative approval, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Any attempt to bypass, defeat or circumvent the Technology Prevention Measures is punishable as a violation of the Technology Acceptable Use Policy and the Student Code of Conduct.

INAPPROPRIATE NETWORK USAGE

To the extent practical, steps shall be taken to promote the safety and security of users of the LISD online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions, and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the Technology Acceptable Use Policy.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

SUPERVISION AND MONITORING

It shall be the responsibility of all professional employees (pedagogical and administrative staff) of LISD to supervise and monitor usage of LISD's computers, computer network and access to the Internet in accordance with these policies: the Technology Acceptable Use Policy and the Children's Internet Protection Act. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Director or designated representatives.

EDUCATION

LISD will advocate and educate employees, students, parents, and the LISD community on Internet safety and "cyber-bullying." Education will be provided through such means as professional development training and materials to employees, PTA presentations, and the LISD website.

CYBER-BULLYING

The LISD Technology Acceptable Use Policy includes provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying. Network users may not use the district's network for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

Network users may not use vulgar, derogatory or obscene language.

Network users may not post inappropriate anonymous messages, or forge e-mail or other messages.

Furthermore, School District computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, State of Texas or local laws. This includes, but is not limited to any threat or act of intimidation or harassment against another person.

ADOPTION

This Internet Safety Policy was adopted by the Lovejoy Independent School District Board of Trustees at a public meeting, following normal public notice, on the 19th day of June 2012.