Technology Acceptable Use Policy

Introduction

Lewis Central CSD recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, we provide access to various technologies, network systems, and internet access for student and staff use. A signed agreement must be on file prior to use of district technologies. Students must have a parent signature as well.

This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- The Lewis Central CSD network is intended for educational purposes. It is not a public access service or a public forum.
- All activity over the network or when using district technologies may be monitored and retained. Access is a privilege, not a right.
- Access to online content and posting of content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students and staff are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Lewis Central CSD makes a reasonable effort to ensure users' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

Lewis Central CSD may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, network systems and internet access.

As new technologies emerge, Lewis Central CSD will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Electronic Resources

The Lewis Central CSD views the use of electronic resources as central to the delivery of its educational program, and as such maintains the expectation that all students will use electronic resources as an essential part of their learning experiences. It is the policy of the Lewis Central CSD to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities by staff and students. The amount of time and type of access available for each student and staff member may be limited by the District's technology and the demands for the use of the District's technology. These procedures are written to promote appropriate and responsible technology use in support of the mission and goals of the Lewis Central CSD and its schools. Although reasonable efforts will be made to make sure students will be under supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students may encounter information that may not be of education value and/or may be inappropriate. It shall be a violation of this policy for any employee, student, or other individual to engage in any activity that does not conform to the established purposes and general rules for the use of electronic resources.

Web Access

Lewis Central CSD provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow district protocol to alert an IT staff member or submit the site for review.

Email

Lewis Central CSD may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

Email accounts should be used responsibly. Users should not attempt to open files or follow links from unknown or untrusted origin. Users are expected to communicate with the same appropriate and courteous conduct online as offline.

Email usage may be monitored and archived. All communications and information accessible via electronic resources should be assumed to be public records and, barring a privilege, they will be disclosed.

Social Networking and Collaborative Content

Recognizing the benefits collaboration brings to education, Lewis Central CSD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate and courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Lewis Central recognizes the importance of social media for its employees, and acknowledges that its employees have the right under the First Amendment, in certain circumstances, to speak out on matters of public concern. However, the Board will regulate the use of social media by employees, including employees' personal use of social media, when such use:

1. Interferes with the work of the school district;
2. Is used to harass co-workers or other members of the school;
3. Breaches confidentiality obligations of school district employees;
4. Disrupts the work of the school district;
5. Harms the goodwill and reputation of the school district in the community; or
6. Violates the law, board policies and/or other school rules and regulations.

Mobile Devices Policy

Lewis Central CSD may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network and are expected to treat these devices with care and caution. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored.

Personally-Owned Devices Policy

Students and staff should keep personally-owned devices (including laptops, tablets, smart phones, and cell phones) put away during school hours—unless being used for educational purposes. Because of security concerns, a separate network may be provided for personally-owned devices.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run an executable program (.exe) over the school network or onto school resources without express permission from IT staff. You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Netiquette

Users should always use the Internet, network resources, and online sites in a respectful manner and realize that among the valuable content online is unverified, incorrect, or inappropriate content. LCCSD is not responsible for the accuracy of information users access on the internet. Users should use trusted sources when conducting research via the Internet.

Users should not post anything online that they would not want parents, teachers, future colleges or employers to see. Once something is posted online, it can be shared in ways not intended and access can become impossible to control.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should be cautious and responsible when providing personal information, including phone number, address, social security number, birthday, or financial information, over the Internet. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. All messages, comments, images, or any online content that threatens personal safety should be brought to the attention of a responsible individual immediately.

Harassment

Harassment will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of harassment. Do not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, harassment can be a crime. Network activity can be monitored and retained indefinitely.

Examples of Acceptable Use

- Creation of files, projects, videos, web pages, podcasts, and other activities using electronic resources, in support of education and research and consistent with the mission of the District.
- Participation in electronic communication and collaboration activities such as blogs, wikis, podcasts, email, and other activities using electronic resources, in support of education and research and consistent with the mission of the District.
- With parent permission, posting of student-created original educational material, curriculum-related materials, and student work. Sources outside the classroom or school must be appropriately cited and all copyright laws must be followed.
- Staff use of electronic resources for incidental personal use in accordance with all District policies and guidelines.
- Connection of any personal electronic device is subject to all guidelines in this document.
- Proper codes of conduct in electronic communication must be used. Providing personal information is inappropriate; when using electronic communications, extreme caution must always be taken in revealing any information of a personal nature.
- All electronic resource accounts are to be used only by the authorized owner of the account for the authorized purpose
- All communications and information accessible via electronic resources should be assumed to be public records and, barring a privilege, they will be disclosed.
- As a representative of your school and community, exemplary behavior while using electronic resources should be practiced.

Unacceptable Use

- Providing unauthorized personal information such as an address or phone number.
- Contributing to cyberbullying, hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors.
- Using profanity, obscenity, racist terms, or other language that may be offensive to another user.
- Any use of the electronic resources for individual profit or gain; for product advertisement; for political action or political activities; or for excessive personal use.
- Playing games, accessing social networking sites, and streaming or downloading audio and video files unless specifically authorized by a teacher for instructional purposes.
- Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting other users on the electronic resources.
- Using an electronic resources account authorized for another person.
- Making use of the electronic resources in a manner that serves to disrupt the use of the network by others.
- Destroying, modifying, or abusing hardware and/or software.
- Unauthorized downloading or installation of any software, including shareware and freeware, for use on Lewis Central electronic resources.
- Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner. Exceptions are made when duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).
- Using electronic resources to access or process pornographic material, inappropriate files, or files dangerous to the integrity of the network. Accessing any material that is inappropriate for minors including products or services that the possession and/or use of by minors is prohibited by law.
- Malicious use of the electronic resources to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.
- Any attempts to defeat or bypass the District's Internet filter by using or trying to use proxies, https, special ports, modification to District browser settings or any other techniques, designed to avoid being blocked from inappropriate content or to conceal Internet activity.
- Using any electronic resources for unlawful purposes.

This is not intended to be exhaustive lists. Users should use their own good judgment when using school technology.

Student Responsibilities

- Students should use emerging communications and collaboration tools to create and personalize networks of experts to inform their education process.
- Students should engage in technology-enabled learning experiences that transcend the classroom walls and are not limited by resource constraints, traditional funding streams, geography, community assets or even teacher knowledge or skills.
- Students should see the use of relevancy-based digital tools, content and resources as a key to driving learning productivity, not just about engaging students in learning.
- Students should protect district laptop computers, tablets and related equipment from damage and theft. Each student will be responsible for any damage to the laptop computer, tablet and related equipment they have been issued from the time it is issued to them until the time it is turned back in to the district.

Staff Responsibilities

- Staff should use emerging and collaboration tools to be most productive and to effectively engage students in significant learning.
- Staff should see the use of relevance-based digital tools, content and resources as a key to driving learning productivity for themselves and their students.
- Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to electronic resources procedures as well as with the mission and goals of the Lewis Central CSD.
- Staff should make reasonable efforts to become familiar with the electronic resources and their use so that effective monitoring, instruction, and assistance may be provided. Staff should report any misuse to their supervisor.
- Staff should protect district laptop computers, tablets and related equipment from damage and theft. Each staff will be responsible for any damage to the laptop computer, tablet and related equipment they have been issued from the time it is issued to them until the time it is turned back in to the district.

Lewis Central District Rights and Responsibilities

The Lewis Central CSD recognizes its obligation to protect the well-being of students and staff in its charge. To this end, the district retains the following rights:

- To log electronic resource use and to monitor fileserver space utilization by users, and assume no responsibility or liability for files deleted due to violation of fileserver space allotments.
- To monitor the use of electronic resource activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review. The District has the right, but not the duty, to monitor any and all aspects of its technology, network systems, and internet access, including, but not limited to sites students and staff visit on the internet and reviewing e-mail.
- To provide internal and external controls as appropriate including the right to determine who will have access to Lewis Central CSD -owned equipment.
- To exclude those who do not abide by the Lewis Central CSD's electronic resources policy or other policies governing the use of school facilities, equipment, and materials. A user account may be closed at any time based upon the District's determination that a user has violated this policy.
- To restrict electronic resource destinations through software or other means every computer in the school district having internet access shall not be operated unless internet access from the computer is subject to a technology protection measure. (i.e. filtering software)
- To provide guidelines and make reasonable efforts to train staff and students in acceptable use and policies governing electronic resource communications.
- To monitor and maintain email distribution lists.

- To use filtering software to block or filter access to visual depictions that are obscene and all child pornography in accordance with CIPA. Other objectionable material may be filtered. The determination of what constitutes "objectionable" material is a local decision determined by the District's educational goals.

Disclaimer

- The Lewis Central CSD cannot be held accountable for the information that is retrieved via electronic resources.
- Even if students have NOT been given access, they may still be exposed to information from the District's computers, network systems, and/or the internet in the guided curricular activities at the discretion of their teachers.
- Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. Network administrators have access to all email and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities. Students and staff waive any right to privacy in anything they create, store, send, disseminate or receive on the District's technology and network systems, including the internet.
- The District reserves the right to monitor, inspect, copy, review, and store without prior notice any and all usage of: the network; user files and disk space utilization; user applications and bandwidth utilization; user document files, folders, and electronic communications; email; Internet access; and any and all information transmitted or received in connection with network and/or email use.
- All such information files shall be and remain the property of the District, and no student or staff user shall have any expectation of privacy regarding such materials. The District reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Iowa.
- Electronic backup is made of email for the purpose of public disclosure requests and disaster recovery. Barring power outage or intermittent technical issues backups are made of staff and student files on District servers for recovery of accidental loss of deleted files. Recovery is not guaranteed.
- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites. While Lewis Central CSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
- The Lewis Central CSD will not be responsible for any damages users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or user errors or omissions. Use of any information obtained is at the user's own risk.
- Lewis Central CSD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.
- The Lewis Central CSD makes no warranties (expressed or implied):
    - The District does not warranty that its technology, network systems or internet access will be secure and free of viruses, spyware and/or malware at all times.
    - The District is not responsible for the content of any advice or information received by a user or any costs or charges incurred as a result of seeking or accepting any information;
    - Any costs, liability, or damages caused by the way the user chooses to use his or her access to the electronic resources are the responsibility of the user. The District will not be responsible for any damages relating to the loss of data, delays, non-deliveries, mis-deliveries or service interruptions caused by negligence or omission.
    - The District is not responsible for the accuracy of information users access on the internet and is not responsible for any unauthorized charges students or staff members may incur as a result of their use of the District's technologies. Any risk and/or damages resulting are assumed by and is the responsibility of the user.
- The Lewis Central CSD reserves the right to change its policies and rules at any time without notification. The interpretation, application, and modification of this policy is within the sole discretion of the District. Any

questions or issues regarding this policy should be directed to the Superintendent, any building principal or the technology coordinator.

Personal Device Warning

By connecting a mobile device to the Lewis Central CSD email system, you acknowledge and agree that the Lewis Central CSD Information Technology Department reserves the right to enforce any security measures deemed necessary to mitigate data leakage and protect students.

This includes but is not limited to:

1. Remotely delete the contents of your mobile device. This may include district and personal contacts, pictures, etc.
2. Enforce the use of a password / pin to access the mobile device.
3. Restrict the use of applications deemed a security risk. In addition, you must understand that documents or records – including electronic communications of a public agency are public records under Iowa state law. Using any personal device or computer for school district business can result in a requirement that you submit your personal device for examination or search if a public records request is received concerning information that may be stored on your personal device.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including, but not limited to:

- Suspension of network, technology, or computer privileges
- Notification to parents/supervisors
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution.

Appropriate disciplinary repercussions will be determined on a case-by-case basis and will be based upon the nature and seriousness of the individual incident.

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____
(Staff Member Printed Name)

_____ _____
(Staff Member Signature) (Date)

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____
(Student Printed Name)

_____ _____
(Student Signature) (Date)

I have read and discussed this Acceptable Use Policy with my child:

_____
(Parent/Guardian Printed Name)

_____ _____

(Parent/Guardian Signature) (Date)