Authorization for Electronic Network Access
AUP and BYOD Policies

DEFINITIONS

BYOD – Bring Your Own Device

AUP – Authorized Use Policy

User includes anyone, including employees, students, and guests, using LeRoy CUSD #2 technology; including, but not limited to, computers, networks, Internet, e-mail, chat rooms, and other forms of technology services and products.

Network is wired and wireless technology networks including school and district networks, cellular networks, commercial, community, or home-based wireless networks accessible to students.

Equipment are cellular phones, "smart phones", PDAs, MP3 players, iPod-type devices, and portable computers such as laptops, iPads, desktops, tablets, and netbooks, as well as portable storage devices.

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. The District's electronic network is part of the curriculum and is not a public forum for general use.

AVAILABILITY OF ACCESS

Electronic networks, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The use of technology whether owned by the District or devices supplied by the Users entails personal responsibility. It is expected that Users will comply with LeRoy CUSD #2 rules, act in a responsible manner, and will honor the terms and conditions set by the classroom teacher, LeRoy Jr/Sr High School, and the District. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies.

LeRoy CUSD #2 reserves the right to monitor Users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network, and/or Internet access or files, including e-mail.

STUDENT DEVICES

School Administration may search a student's memory device, cellular phones, "smart phones", PDAs, MP3 players, iPod-type devices, and portable computers such as laptops, iPads, desktops, tablets, and netbooks, as well as portable storage devices, if they feel school rules have been violated, which may include, but are not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, or other issues regarding bullying, etc.

Students may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from both a staff member and those whom they are recording.

A student-owned device is a non-district supplied device used while at school or during school or district-sponsored activities. Students may use student-owned devices in class only with the teacher's expressed permission.

Use of a device without direction of the teacher may result in suspension or termination of privileges and other disciplinary action consistent with District policies.

CYBERSAFETY AND CYBERBULLYING

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,

4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Despite every effort for supervision and filtering, all Users and Students' parents/guardians are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every User must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every User must report security or network problems to a teacher or administrator.

GOOGLE APPS

LeRoy CUSD #2 is offering students a free educational suite of applications for use to enhance teaching and learning. Google Apps is a concept known as "cloud computing" where services and storage are provided via the Internet. The District is providing students Google Message Security, which is a service that provides system administrators the capability to limit messages based on where they are from, where they are going, or the content they contain. The District will use this technology protection measure to filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the Internet.

Students will have the opportunity to receive access via an @leroyschools.org e-mail address, not a traditional @gmail.com address. The Google Apps for Education allows us to limit e-mails to file sharing between students and teachers that have only the @leroyschools.org address extension. While students and teachers can access their @leroyschools.org account and documents anywhere, anytime, they can only send and receive e-mails to and from the @leroyschools.org address extensions (ie, students cannot send or receive e-mails to or from e-mail addresses such as @hotmail.com, @gmail.com, @leroyk12.org, etc).

In addition to these extensive restrictions, all exchanges between students-teachers, teachers-students, and students-students are automatically stored for our access. Accounts are monitored to ensure appropriate use, but we also rely on students, teachers, and parents to help us intercept misuse. The purpose of Google Apps for Education is solely for educational purposes. Any other use is in violation of the district's Authorized Use Policy (AUP), which all parents sign at registration and is available on our website.

In order for students to gain access to Google Apps for education, LeRoy CUSD #2 must obtain parental permission as per the Child Online Privacy Protection Act (COPPA). COPPA is a regulation that requires parental consent for the online collection of information about users under 13.

INTERACTIVE WEB 2.0 TOOLS

Online communication is critical to the students' learning of 21st Century Skills, and tools, such as blogging, podcasting, and chatting, offer an authentic, real-world vehicle for student expression. Web 2.0 tools include the use of Google Apps, District Moodle, blogs, podcasts, or other 2.0 tools. Users may be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the District. Teachers may recommend and use public interactive sites that, to the best of their knowledge are legitimate and safe. As the site is public and the teacher, school, and District are not in control of it, all students must use their discretion when accessing information, storing, and displaying work on the site.

TERMS AND CONDITIONS

These are examples of inappropriate activity on the LeRoy CUSD #2 network, but the District reserves the right to take immediate action regarding any activities 1) that create security and/or safety issues for the District network, Users, schools, network or computer resources; 2) that expend District resources on content it determines lacks legitimate educational content/purpose; or 3) other activities as determined by the District as inappropriate.

1. Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.

2. Criminal activities that can be punished under the law.

3. Selling or purchasing illegal items or substances.

4. Obtaining and/or using anonymous e-mail sites, spamming, or spreading viruses.

5. Causing harm to others or damage to their property.

6. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.

7. Deleting, copying, modifying, or forging other Users' names, e-mails, files or data, disguising one's identity, impersonating other users, or sending anonymous e-mail.

8. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.

9. Using any computer/mobile devices to pursue “hacking”, internal or external to the District, or attempting to access information protected by privacy laws.

10. Accessing, transmitting, or downloading large files.

11. Using websites, e-mail, networks, or other technology for political uses or personal gain.

12. Users must not intentionally access, create, store, or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile, or that harasses, insults, or attacks others.

13. Advertising, promoting non-District sites or commercial efforts and events.

14. Users must adhere to all copyright laws.

15. Users are not permitted to use the network for non-academic related bandwidth intensive activities, such as network games or transmission of large audio/video files or serving as a host for such activities.