Student Use of LPSD Technology Resources, the Internet, and Communication Systems[1] Policies

The purpose of this policy is to inform parents, guardians and students of the rules governing the use of district and personal technology resources while on school property, in school vehicles, and at school-sponsored activities, as well as the use of district technology resources via off-campus remote access.

Introduction

Lewis-Palmer School District (LPSD) is pleased to offer students access to district computers, communication systems, the Internet, and other technology resources to promote educational excellence. Each student is responsible for her/his use of technology, whether personal or district-provided. While using technology resources on school property, in school vehicles, and at school-sponsored activities, as well as using district technology via off- campus remote access, each student must act in an appropriate manner consistent with school rules, Board policy, and applicable law. It is the joint responsibility of school personnel and the parent/guardian of each student to educate the student about his/her responsibilities and to establish expectations when using district technology.

Using LPSD technology resources, the Internet, and communication systems

District technology resources are provided to students to conduct research, complete assignments, and communicate with others in furtherance of their education. Access is a privilege and not a right; as such, general rules of school behavior apply. Access to these services is given to students who agree to act in a considerate and responsible manner. Just as students are responsible for good behavior in a classroom or a school hallway, they must also be responsible when using technology resources and networks.

Use of the Internet and communication systems require students to think critically, analyze information, write clearly, use problem-solving skills, and hone technology and research skills that employers demand. Use of these tools also encourages an attitude of lifelong learning and offers an opportunity for students to participate in online learning activities, ask questions of and consult with experts, communicate with other students and individuals, and locate materials to meet educational and personal information needs.

Students are expected to use all technology resources in a manner consistent with this policy and will be held responsible for their intentional misuse.

Content filtering

The Board believes the educational opportunities inherent in technology tools outweigh the possibility that users may procure material not consistent with the educational goals of the district. However, the Internet and communication systems are fluid environments in which students may access materials and information from many sources, including some that may be inappropriate for students.

Some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, profane, sexually oriented, or potentially offensive. While the intent is to make Internet access available to further educational goals and objectives, students may find ways to access these other materials as well. LPSD does not condone or permit the use of these materials and uses content filtering mechanisms to protect students to the extent reasonably possible.

To protect students from material and information that is obscene, child pornography, or otherwise harmful to minors, as defined by the Board, Internet traffic is monitored and filtered in accordance with applicable law. Students shall report, to the supervising staff member, access to material and information that is obscene, pornographic, inappropriate for minors or otherwise in violation of this policy. If a student becomes aware of other students accessing such material or information, he/she shall immediately report it to the supervising staff member.

Parents and guardians must be aware that content filtering tools are not completely fail-safe and, while at school, direct supervision by school personnel of each student using a computer is desired but not always possible. Students shall take responsibility for their own use of personal and/or district technology resources, the Internet, and communication systems to avoid contact with material or information that may be harmful to minors. Whether using personal or district devices, students are encouraged to utilize district networks when on district property. The district is unable to content filter non-district networks.

Privacy

LPSD computers and communications systems are owned by the district and are intended for educational purposes at all times. Students shall have no expectation of privacy when using district technology resources. All digital storage systems are district property. Network administrators may review files and communications to maintain system integrity and ensure that technology is used responsibly. Students should not expect that files stored on district resources will be kept private. The district will adhere to all federal and state laws regarding personally identifiable information.

The district reserves the right to monitor, inspect, copy, review, and store (at any time and without prior notice) all usage of district computers and computer systems, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through district computers and computer systems shall remain the property of the school district.

Proper and acceptable use of all technology resources

All district technology resources, including but not limited to district computers, communications systems, and the Internet, must be used in support of education and academic research and must be used in a manner consistent with the educational mission and objectives of LPSD and this policy. A list of technological resources used is made available on district web sites.

Activities that are permitted and encouraged include:
- School work
- Original creation and presentation of academic work
- Research on topics being studied in school
- Research for opportunities outside of school related to community service, employment, or further education.

Activities that are not permitted when using district or personal technologies on school property, in school vehicles, at school-sponsored activities, or via off-campus remote access include but are not limited to:
- Plagiarism or representing the work of others as one's own without express consent
- Promotion of violence or destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
- Items containing pornographic, obscene, or other sexually oriented materials
- Language/action that is profane, harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons with regard to race, color, sex, religion, national origin, age, marital status, disability, or any other status protected by law
- Perpetuating something that is knowingly false or could be construed as intending to purposely damage another person's reputation
- Representing Copyright ©, Registered ®, and/or Trademark ™ materials as one's own work
- Searching, viewing, communicating, publishing, downloading, storing, or retrieving materials that are not related to school work, community service, employment, or further education (thus, searching inappropriate materials is not permitted)

- Vandalism, including intentionally damaging or modifying technology or networks
- Using another individual's Internet or digital account
- Impersonating another or transmitting through an anonymous remailer
- Intentional or neglectful transmission of viruses or other destructive files
- Subscription to any unsanctioned online services or ordering of any goods or services
- Unsanctioned online sharing of any student's name, home address, phone number or other personal information
- Unsanctioned uses of technology (e.g.: games, role-playing multi-user environments, gambling, junk mail, chain mail, jokes, or raffles)
- Unsanctioned participation in online chat rooms or using instant messaging, unless specifically assigned by a teacher
- Use of district resources for personal financial gain, political purposes, or fraud
- Unsanctioned use of district resources for commercial transactions or advertising
- Attempting to gain unauthorized access to technology resources
- Intentionally bypassing district filters
- Any activity that violates a school rule, a district policy, or a local, state, or federal law.

Students are expected to report harassment, threats, hate-speech and inappropriate content to a teacher or administrator. If a student has questions about whether a specific activity is permitted, he/she shall ask a teacher or administrator.

Security

Students must use district technology resources responsibly and in a secure manner.

Security on district technology resources and communication systems is a high priority. Students who identify a security problem while using district technology resources must immediately notify a teacher or administrator. Students should not demonstrate the problem to other users except as needed to report it to the appropriate teacher, administrator, or technician. Logging on to the Internet or communications systems as another user or system administrator is prohibited.

In the interest of student safety and security, the district shall educate students about appropriate online behavior, including cyberbullying awareness and response, interacting via social media, and positive use of digital communication tools.

Students must not share their logins, passwords, or access with others.

Online assessments

Student assessments may be conducted using a variety of technologies.

Normally, students will use these technologies as a part of their instruction, and student data will be protected by applicable privacy policies.

Vandalism

Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse, or disrupt operation or any network within the school district or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or district-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses.

Any intentional act to district technology resources, communications systems, or datathat requires a person's time to repair, replace, or correct is also considered vandalism.

District software

Only authorized software may be installed on district-owned technology resources and networks. All software must be approved before being installed by a district technology services technician. Students are not permitted to download or install software on district-owned equipment.

Assigning student projects and monitoring student use

The district will make every reasonable effort to see that district technology resources, the Internet, and communication systems are used responsibly by students. Administrators, teachers, and staff have a professional responsibility to work together to monitor students' use of technology, to help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information and tools to meet their educational goals. Students shall have specifically defined objectives and strategies prior to accessing material and information via technology.

Consequences of misuse

Misuse of personal or district technology resources while on or near school

property, in school vehicles, and at school-sponsored activities, as well as the use of district technology resources via off-campus remote access, may result in disciplinary action up to and including expulsion. This policy shall be used in conjunction with other Board policies. In addition, the student's use of district technologies may be suspended or restricted. A school may temporarily hold (pending parental or same-day pick up) personal technology resources that are used inappropriately. Individual schools may choose to have additional rules and regulations pertaining to the use of personal, networked, and communication resources in their respective buildings. Furthermore, intentional unauthorized access and/or damage to networks, servers, user accounts, passwords, and other technology resources may be punishable under applicable law.

Reliability and limitation of liability

LPSD makes no warranties of any kind, expressed or implied, related to the use of district technology and technology systems, including access to the Internet and communications systems. LPSD will not be responsible for any damages suffered by the student, including, but not limited to, those arising from non-deliveries, misdeliveries, service interruptions, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or other technologies is at the student's own risk. LPSD specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. The student and his/her parent or guardian will indemnify and hold LSPD harmless from any losses sustained as the result of misuse of the district's technology resources by the student.

Students and parents/guardians shall be required to sign the district's Network and Technology Equipment User Agreement before Internet or communication systems accounts shall be issued or access shall be allowed.

Adopted: June 17, 2007
Revised: May 17, 2012
Revised: July 29, 2012
Revised: May 19, 2016
Revised: September 14, 2017

LEGAL REFS:
20 U.S.C. 6751 *et seq.* (Enhancing Education Through Technology Act of 2001)
47 U.S.C. 254(h) (Children's Internet Protection Act of 2000)
47 C.F.R. Part 54, Subpart F (Universal Support for Schools and Libraries)
C.R.S. § 22-87-101 et seq. (Children's Internet Protection Act)

Lewis-Palmer School District #38, El Paso County, Colorado