RED LION AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET AND NETWORK FACILITIES

ADOPTED: January 16, 1997

REVISED: July 18, 2013

	815. ACCEPTABLE USE OF INTERNET AND NETWORK FACILITIES
1. Purpose	In a free and democratic society, access to information is a fundamental right of citizenship. Digital literacy is essential for student success. Appropriate technology tools and network resources are made available to students and staff to increase engagement through fostering creativity, enhancing productivity, facilitating research and promoting communication and collaboration with others in an educational setting. The Board of School Directors of the Red Lion Area School District (Board) supports the use of the Internet, information technology, district and personally owned devices, and other network facilities in the district's instructional programs in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration. Use of the district's information technology tools and network facilities shall be consistent with and in furtherance of the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. The changing educational environment and level of technology integration may require that students access web-based resources while using district or personally owned equipment. The use of technology tools, websites, and resources, for the purpose of completing curricular objectives, is a privilege, not a right. Any web-based, personally owned user accounts created by district personnel or by the end-user for the purpose of completing activities associated with course curricula or other school related functions are subject to the guidelines defined by the Acceptable Use Policy of the Red Lion Area School District, regardless of where the access to that resource has taken place.
2. Definitions 18 U.S.C. Sec. 2256	**Child Pornography** - any visual depiction, including any photograph, film, video, picture or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where: (1) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (2) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (3) such visual depiction

	has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. **Hacking** - any attempt to gain unauthorized access (or the unauthorized access) to network facilities or using district network facilities to attempt or to gain unauthorized access to other networks or computing resources.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Harmful to Minors** - any picture, image, graphic image file, or other visual, sound or written depiction that: 1. Taken as a whole, and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion. 2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for 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. 3. Lacks serious literary, artistic, political or scientific value as to minors. 4. Depicts extreme violence. 5. Promotes intolerance. **Illegal Activities/Uses** - any use of network facilities which violates a municipal ordinance, or local, state, or federal law, including those activities relating to intellectual property rights, trade secrets, the distribution of obscene or pornographic materials, or the Family Educational Rights and Privacy Act. **Information Technology** - any electronic device, computer hardware and software, operating systems, web-based information and applications, telephones and other telecommunications products, video equipment and multimedia products, and office products such as photocopiers and fax machines. Examples of information technology tools includes, but is not limited to, such devices as cell phones, smart phones, tablets, eReaders, laptop computers, PDA's, iPods or other electronic music players, etc. When used in this policy, *information technology* is sometimes referred to as information technology tools or tools. **Network Facilities** - 1. Computer hardware and software, electronic connections, electronic devices and other information technology tools used for information processing as well as peripheral devices connected to these tools. 2. Network bandwidth including Internet bandwidth and other devices necessary to facilitate network connectivity such as e-mail services, fileservers, routers,

	switches, hubs, firewalls, premise wiring, network data ports, etc. 3. Computers hardware and software, electronic connections, electronic devices and other information technology tools used on district property or used off district property that impacts the district, or causes a disruption to the educational environment, or when such use comes in conflict with the Student Code of Conduct or district Policy, whether or not such tools are owned by the district and whether or not they are connected physically or wirelessly to the district's information network(s). 4. Computers, electronic connections, electronic devices and other information technology tools while they are connected remotely (from home or elsewhere) to the district's network. **Obscene** – material which: to the average person, applying contemporary community standards, appeals to the prurient interest; depicts or describes in a patently offensive way, sexual conduct described by law to be obscene; and taken as a whole, lacks serious literary, artistic, political, educational or scientific value. **Online Collaboration** - using site-based or web-based technology tools to communicate and work productively with other users to complete educationally relevant tasks.
47 C.F.R. 54.520	**Technology Protection Measure** – a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors. **Technology Tools -** including, but not limited to, hardware, software, web-based applications (e.g. Google Apps for Education, Gmail, Wikispaces.com, Blackboard, Blogs, Discussion Boards, Podcasts, etc.) electronic devices, telecommunication products, audio/video equipment, and other tool used for classroom instruction.
3. Authority	The Board establishes that use of district or personally owned information technology tools and network facilities impacting the district is a privilege, not a right. Users have **no expectation of privacy or confidentiality** in the content of electronic communications, Internet access, or other computer files sent and received utilizing the districts' information technology tools, network facilities or stored in his/her fileserver space utilization by users, while respecting the privacy rights of outside users. District network administrators have the right to deny, revoke, or suspend specific use of its information technology resources. The district's Superintendent, or other authorized school employees, may at any time, review the subject, content, and appropriateness of electronic communications, Internet access, usage of the district's information technology or other computer files

	and remove them or block the inappropriate use as warranted, or report any violation of these rules to the district's administration or appropriate law enforcement officials. The district reserves the right to remove a user account from its network facilities to prevent further unauthorized or illegal activity if this activity is discovered. The district has the right to monitor, inspect, copy, review and store at any time, without prior notice, any and all usage of its information technology, network facilities and internet usage and any and all information transmitted or received in connection with such usage. All such information files and user accounts shall be and remain the property of the district. The building administrator shall also have the authority to determine what is inappropriate use of the district or personally owned information technology and district network facilities.
4. Delegation of Responsibility	Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to utilize and discriminate among information sources, to identify information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. <u>The school district will annually educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.</u> When using district or personally owned information technology tools and district network facilities, students and staff have a responsibility to respect and protect the rights of every other user in the district and of those they communicate or interact with on the Internet. This includes maintaining the integrity of district approved email or communication systems.
24 P.S. Sec. 4601 et seq	The district shall provide a copy of this policy to parents/guardians, upon written request or via the district web site.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The Superintendent or designee shall be responsible for implementing procedures to determine whether the district's information technology and network facilities are being used for purposes prohibited by law and this policy, or for accessing sexually explicit materials. The procedure shall include, but not be limited to: 1. Requiring the utilization of a technology protection measure that blocks or filters user's Internet access to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board. 2. Maintaining and securing a usage log. 3. Monitoring and storing information related to online activities of minors and all

	other users.
5. Guidelines	Network accounts or other information technology based accounts shall be used only by the authorized owner of the account for the approved purpose. All communications and information accessible via the district or personally owned information technology or district network facilities should be assumed to be the private property of the district and shall not be disclosed. The district reserves that right to impose network, Internet, and/or printing restrictions on any or all users. <u>Prohibitions</u> Users are expected to act in a responsible, ethical, and legal manner, and in accordance with district policy, accepted rules of network etiquette, and federal, state, and local law. Specifically, the following uses of district or personally owned information technology tools and network facilities are prohibited: 1. Facilitating illegal or inappropriate activity on or by network facilities, or activities done on network facilities to facilitate an illegal or inappropriate act or purpose. 2. Commercial, for-profit, or political purposes, including gambling, lobbying, soliciting sales, advertising, selling, servicing, or conducting any other business-related activities using district resources that are not for the benefit of or associated with the operation of the district. 3. Non-work or non-school related work, except where permission is granted via policy, building guidelines, or administrative approval. 4. Uploading, creating, or attempting to create a computer virus or other inappropriate or damaging information technology tool exploitation or misappropriation. 5. Hate mail, discriminatory remarks, bullying or threatening, antisocial, offensive, or inflammatory communications or postings. 6. Violating copyright laws, including unauthorized or illegal installation, distribution, plagiarism, reproduction, copying, modification, forwarding, downloading or use of copyrighted materials and fraudulent copying. Copyrighted materials include, but are not limited to, games, stories, encyclopedia entries, or software written by another. Any data uploaded to or downloaded from network facilities are subject to fair use guidelines. 7. Accessing, storing, sending, receiving or transmitting obscene, inappropriate, or

SC 1303.1-A
Pol. 249

Pol. 814

pornographic materials or text files, child pornography, or material or text files, harmful to minors or potentially dangerous to the integrity of the local area network, the district's information technology tools, or its network facilities, as determined by Board policy.

8. Accessing or transmitting files dangerous to the integrity of the district's information technology or network facilities.

9. The use of inappropriate language or profanity while utilizing district network resources. Such mediums would include blogs, discussion forums, texts, email, files, usernames, passwords, etc.

10. Transmitting sound, pictures, or text likely to be offensive or objectionable to recipients or in violation of the student code of conduct for inappropriate behavior.

11. Intentional obtaining or modifying of files, passwords, data, or information belonging to other users.

12. Impersonating another user, including, but not limited to, by using another's email address, user account, or password, or using anonymity or pseudonyms.

13. Violating software or other licensing agreements.

14. Loading, installing, previewing, copying, or using of unauthorized games, programs, files, software, or other electronic media.

15. Transmitting or creating any digital content disruptive to the instructional process or threatening to another district user whether or not the district's information technology or network facilities are used to facilitate, send or receive any such transmission.

16. Destruction, modification, abuse or unauthorized access to the district's information technology or network hardware, software and files.

17. Quoting of personal communications in a public forum without the original author's prior consent.

18. Engaging in or accessing chat rooms, discussion forums/boards or instant messaging without the permission or direct supervision of a teacher or administrator.

19. Attempting to circumvent or disable any filter, information security, or other security measure.

20. Attempting to use network facilities while access privileges are suspended or

18 Pa.C.S. § 5703	revoked. 21. Reading, deleting, copying or modifying the email or files of other users or deliberately interfering with the ability of other users to send or receive email. 22. Invading the privacy of other persons. 23. Using the network facilities or information technology to access, send, create, or post material or communications that are damaging to another persons reputation, abusive, obscene, sexually-oriented, threatening, contrary to district policy on harassment, or illegal. 24. Revealing personal information or passwords related to any users on the network other than by district staff in the performance of assigned duties. 25. Hacking, keystroke logging, port scanning, unauthorized attempts to access network resources, creating malicious code, phishing, or spamming. 26. Failing to report a violation of this policy. 27. Use of any social networking or communication medium, on or off-campus, that causes, or could be reasonably expected to cause, a substantial disruption to the educational environment. 28. Taking pictures, video, or audio of individuals without their knowledge or consent and/or relevance to district curricular, co-curricular or extra-curricular activities. 29. Attaching personal technology devices to the network without following the rules detailed in the district's personal devices guidelines, Policy 237, and faculty or student handbooks. 30. Using a non-district network as a means to connect personally owned devices to the Internet in order to circumvent filtering or the guidelines set forth in the Acceptable Use Policy. Per Policy 237, the use of personal technology devices is permitted on District-designated and provided networks only. All use of personal technology devices must be in accordance with Policy 237. All users who connect to permitted networks agree to the requirements of the Responsible Use of Internet and Network Resources policy and should consider his/her personal device subject to the same level of monitoring and access as any District-owned technology device. The District reserves the right to monitor Internet and network use on District guest networks.

31. All cell phones, smart phones, and other prohibited electronic devices are not permitted in classrooms during any administration of Pennsylvania State Assessments. Violation of this rule will result in disciplinary action, and the student will not receive a score on the assessment.

Employee User Specific Guidelines

1. District assigned laptops and related equipment remain the property of the district and employees shall abide by the district's Acceptable Use Policy, regardless of where such use takes place. Users have no expectation of privacy related to the assigned equipment. All data and content stored on the laptop shall be the property of the district.

2. Use of the filter override for the express purpose of accessing sites that are prohibited by this policy is prohibited.

3. In order to maintain appropriate student-employee boundaries, current students who are not relatives, should not be allowed to post or become members of any employee's social networking site, including but not limited to Facebook, MySpace, Twitter, etc. Employees are prohibited from interacting or communicating with students on such sites. Further, personal social networking sites are in the public domain and thereby must comply with the applicable law and code of professional practice and conduct for educators, as established by the PA State Department of Education.

4. Under no circumstances is it permissible to utilize personal technology devices, to willfully access content that is expressly prohibited by the Acceptable Use Policy, Faculty Handbook, or the code of professional practice and conduct for educators, as established by the PA State Department of Education.

Safety And Security

To the greatest extent possible, users of the district's network will be protected from harassment and unwanted or unsolicited communication while using district resources. To protect the integrity of network facilities and the safety of users, the following guidelines shall be followed:

1. The security of network facilities is protected through the use of passwords. Users shall not reveal their passwords to another individual or use any other user's password. If a user suspects someone else has his/her password, s/he shall change it immediately and notify the district. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files.

2. Users are not to use a computer that has been logged in under another user's name.

	3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. 4. Users shall notify the district of any change in passwords, violation of this policy, or other security risk. 5. Any network user who receives threatening or unwelcome communications shall immediately report them to a teacher or administrator. 6. Network users shall not reveal personal information to other users on the network, including through chat rooms, email, Internet, etc. that could identify themselves or other users, or allow a person to locate a user. 7. Users shall not intentionally seek information on, obtain copies of, or modify files, other date, or passwords belonging to other users. 8. Users shall report Internet contacts which attempt to arrange a face-to-face meeting with any user to a supervising teacher or administrator. 9. Users shall not transfer or download confidential data or data that contains sensitive personally identifiable information via flash drives, thumb drives, or such other portable storage devices. <u>Consequences For Inappropriate Use</u>
Pol. 218	Inappropriate, unauthorized, or illegal use or violation of this policy will result in appropriate disciplinary action for both students and staff, which could include, but are not limited to, the cancellation of privileges or notification of the appropriate legal authorities (for violation of federal, state or local law). Inappropriate, unauthorized, or illegal use or violations of the prohibitions by a student user shall make the student subject to the disciplinary provisions of the Code of Student Conduct. Any such actions would be subject to applicable procedures established by the district. Any user identified as a security risk or having a history of problems with other computer systems may be restricted from access to the network, ranging from limited access to complete denial of access.

18 Pa. C.S.A. Sec. 7611 et seq	The district will report any illegal uses of its information technology or network resources to the appropriate legal authorities, as some violations may be subject to prosecution under Pennsylvania criminal statutes or liability under civil statutes. Offenders may be subject to criminal prosecution for activities such as, but not limited to, illegal use of the network, intentional deletion or damage to files of data belonging to others, copyright violations, theft of services, accessing, altering, or damaging any computer system, network, software or database, with an intent to interrupt the normal functioning of an organization, disclosing a password to a computer system, network, intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software. District technology tools and personally owned electronic devices may be confiscated and subject to search consistent with applicable law and policy and in consultation with the District Solicitor. District employees should be aware that files and electronic communications may be discoverable under law, including the Right to Know Law. District employees shall be subject to discipline, up to and including termination, for violation of this policy or federal state or local law in accordance with Board policies. Any act of vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses. The district's information technology or network facilities users shall be responsible for damages to the network facilities, including equipment, systems, and software resulting from deliberate or willful acts. <u>Filtering</u>
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software. The district will also monitor online activities of users through direct observation or technological means, to ensure adherence to this policy. Internet filtering software or other technology based protection systems may be disabled by the Director of Technology or his/her designee, as necessary, for purposes of valid research or other educational projects being conducted by users, as determined and approved by a building administrator. Every district computer used by student and staff shall be equipped with Internet blocking/filtering software.
47 U.S.C. Sec. 254	Internet safety measures shall effectively address the following: 1. Control of access by minors to inappropriate content on the Internet. 2. Safety and security of minors when using email, chat rooms, and other forms of direct communications.

3. Prevention of unauthorized online access, including "hacking" and other unlawful activities.

4. Unauthorized disclosure, use, and dissemination of personal information.

5. Restriction of minors' access to materials harmful to them.

6. Restriction of access to visual depictions that are obscene, child pornography or harmful to minors.

Disclaimer Of Warranties/Indemnification

The district makes no warranties of any kind, either express or implied, in connection with this policy, access to and use of its information technology, or network facilities. The district shall not be responsible for any claims, losses, damages or costs (including fees) of any kind suffered, directly or indirectly, by any user of his/her parents(s)/guardians(s) arising out of the use of its information technology or network facilities under this policy. Further, the district is not responsible for damage that may occur as a result of an individual user attempting to connect a personal technology device to any district owned device. By signing this policy, the user is taking full responsibility for his/her use, and the user who is eighteen (18) or older, or in the case of a user under eighteen (18), the parents(s)/guardian(s) are agreeing to indemnify and hold the district administrators professional employees, and staff harmless from any and all losses, cost claims or damages resulting from the user's access to its network facilities, including, but not limited to, any fees or charges incurred through purchases of goods or services by the user. The user, or if the user is a minor, the user's partner(s)/guardian(s) agree to cooperate with the district in the event of the district's initiating an investigation of a user's access to the computer network and the Internet.

References:
School Code – 24 P.S. Sec. 1303.1-A

State Board of Education Regulations – 22 PA Code Sec. 403.1

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

Board Policy – 218, 249, 814PA Wiretapping and Electronic Surveillance Control Act – 18 Pa.C.S. § 5703