No.815A
SECTION: OPERATIONS

TITLE: Student Internet, E-Mail and Network Resources Access Agreement
ADOPTED: June 17, 2002

REVISED: July 18, 2011
May 21, 2012

Lebanon School District

Introduction and Overview	Access to information technologies is integral to the educational mission and purpose of the Lebanon School District. We utilize technology in nearly every facet of instruction, activity, service, research, and operation of our district. This policy provides expectations for the use of technology as it affects our district and educational community. The district's computer network is provided for educational purposes, not as a public access service. Because of the evolutionary nature of technology, it is imperative for students to realize that our policies regarding the use of technology in our community will also be evolutionary. We ask all students to employ their best judgment when it comes to the use of district technology and keep in mind that our policies related to technology are not meant to supersede our other district policies, but rather to compliment them. Although our district provides certain technologies, we recognize that members and guests of our community also have their own technology devices that they bring to our campus and district events. Our policies address the appropriate use of both technologies provided by the district and personally owned technological devices. Please read the policies below before using our network and computers, because by using our technology you agree to be bound by the terms, conditions and regulations below. This policy applies only to students. All adult users including teachers, student teachers, parents, faculty members, and staff members have a separate Technology Use Policy. All children and teens visiting our campus are also subject to the terms and conditions of this Technology Use Policy. No policy can detail all possible examples of unacceptable behavior related to technology use. Our district technology users are expected to understand that the same rules, guidelines, and policies that

	apply to non-technology related student behavior also apply to technology-related student behavior. Our district technology users are expected to use their best judgment when it comes to making decisions related to the use of all technology and the Internet. If there is ever an issue about which you are unsure, ask a member of the Technology Services Department for assistance.	1 2 3 4 5 6 7 8 9
Technology as a Privilege	The use of district and personally owned technology on district property or at district events is a privilege not a right. This privilege comes with personal responsibilities and if you violate the responsible use of any district technologies, your privilege may be revoked and/or suspended.	10 11 12 13 14 15 16
	Our district provides sufficient information technology resources for each student for regular academic pursuits. If a particular research project requires additional resources, the Technology Services Department works with teachers and/or students on a case-by-case basis to provide additional resources.	17 18 19 20 21 22 23
Privacy	The district reserves the right to monitor and track all behaviors and interactions that take place online or through the use of technology on our property or at our events. We also reserve the right to investigate any reports of inappropriate actions related to any technology used at school. All e-mails and messages sent through the district's network or accessed on a district computer can be inspected. Any files saved onto a district computer can also be inspected. Students have a limited expectation of privacy when using their own technology on district property or at district events so long as no activity violates policy, law and/or compromises the safety and well-being of the school community.	24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
Filtering	Our district adheres to the requirements set forth by the United States Congress in the Children's Internet Protection Act. This means that all access to the Internet is filtered and monitored. The district cannot monitor every activity, but retains the right to monitor activities that utilize district owned technology. By filtering Internet access, we intend to block offensive, obscene, and inappropriate images.	40 41 42 43 44 45 46 47 48 49
Right to Update	Since technology is continually evolving, our district reserves the right to change, update, and edit its	50 51 52 53

	technology policies at any time in order to continually protect the safety and well-being of our students and community. To this end, the district may add additional rules, restrictions, and guidelines at any time.	1 2 3 4 5 6 7
Termination of Accounts and Access	Upon graduation or other termination of your official status as a student at our institution, you will no longer have access to the district network or files stored on the district network. In addition, all district owned equipment must be returned prior to student departure. Prior to graduation, we recommend saving all personal data stored on district technology to a removable hard drive.	8 9 10 11 12 13 14 15 16 17
Definitions and Terms Section	Bandwidth is a measure of the amount of data that can be transmitted in a fixed amount of time. Cyber-bullying is when someone sends derogatory or threatening messages and/or images through a technological medium in an effort to ridicule or demean another. Cyber-bullying also takes place when someone purposefully excludes someone else online. For example, a group of students create a group on Facebook that many would like to join, but the student creators purposefully exclude one individual or certain individuals and do not let them join their group. Cyber-bullying also takes place when someone creates a fake account or website criticizing or making fun of another. The Internet connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. The district's network is defined as our computers and electronic devices such as printers, fax machines, scanners, etc. that are connected to each other for the purpose of communication and data sharing. Under this policy, technology is a comprehensive term including, but not limited to, all computers, projectors, televisions, DVD players, stereo or sound systems, digital media players, gaming consoles, gaming devices, cell phones, personal digital assistants, CDs, DVDs, camcorders, calculators, scanners, printers, cameras, external and/or portable hard drives, modems, Ethernet cables, servers, wireless cards, routers and the Internet. District technology refers to all technology owned and/or	18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53

	operated by the district. For the purposes of this policy, user is an inclusive term meaning anyone who utilizes or attempts to utilize, whether by hardware and/or software, technology owned by the district. This includes students, faculty members, staff members, parents, and any visitors to the campus. For the purposes of this policy, personally owned device user refers to anyone who utilizes their own technology on property owned or controlled by the district or at a district sponsored event. PDA stands for personal digital assistant, which is an electronic device, which provides some of the functions of a computer, a cell phone, a music player, and a camera.	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Acceptable Uses Section	Purposes and Use Expectations for Technology The use of all district-owned technologies including the district network and its Internet connection is limited to educational purposes. Educational purposes include classroom activities, career development, communication with experts, homework, and limited high quality self-discovery activities. Commercial and recreational use of district technology resources is prohibited. Students may not utilize district technology to sell, purchase, or barter any products or services. Students may not utilize district technology to play games, visit social networking websites, send instant messages, or e-mails unrelated to the educational purposes stated above. The district is not responsible for any damages, injuries, and claims resulting from violations of responsible use of technology. Personal Responsibility We expect our students to act responsibly and thoughtfully when it comes to using technology. Technology is a finite, shared resource offered by the district to its students. Students bear the burden of responsibility to inquire with their teacher, school administrator or the Technology Services Department when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.	21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53

	District Provided Technology Resources	1
		2
	Network storage is a finite district resource and we expect students to be respectful of other users and limit the amount of space and memory taken up on district computers and on the district network.	3 4 5 6
		7
	This Lebanon School District has a wireless network that is password protected. If you desire to connect your laptop or hand held device to the Internet, you must contact a member of the Technology Services Department. Unauthorized access is forbidden.	8 9 10 11 12
		13
	Only Technology Services Department personnel may connect computers and devices to the district's Ethernet ports and disconnect computers and devices currently connected to the district's network.	14 15 16 17
		18
	The district provides individual technology accounts for students in grades 6 - 12 to keep track of their technology use. Users must log off when they are finished using a district computer. Failing to log off may allow others to use your account, and students are responsible for any activity that occurs through their personal account.	19 20 21 22 23 24 25
		26
		27
Unacceptable Uses of Technology	Mobile Devices	28
	Students need to follow the guidelines in their student handbooks. Cell phones, smart phones and PDA's are permitted on campus, but are not to be used during academic hours without teacher permission. At the elementary and middle school levels, cell phones, smart phones, and PDA's are not permitted to be used throughout the school day without specific permission. At the high school level, students have more privileges regarding such items, as described in the student handbook. It should be noted that the district is not responsible for cell phones, smart phones and PDA's that students elect to bring to school. Students bring such items at their own risk. They should be clearly marked with the student's name and grade.	29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
		44
	Students are not permitted to send text messages with their phones, PDA's or other similar devices without staff permission.	45 46 47
		48
	Students are not permitted to access the Internet with their phones, PDA's or other similar devices using a non-district provided network, including cell phone networks.	49 50 51 52
		53

Recording, Video, and Photography

Students are not permitted to take photographs or video with their phones on district property or at district events without advanced permission from the district.

Students are not permitted to transmit/send any digital media while on district property with their personal devices without permission from the district.

Students are not permitted to use web cams on campus, without specific, prior permission from school administration and the Technology Services Department.

Students may not bring or utilize recording devices or similar data capturing devices or technology on campus without specific permission from a district administrator.

Social Networking and Website Usage

Students may have social networking profiles or accounts, but social networking websites may not be accessed through the district's technology at any time.

Students are not permitted to access any photography sharing websites from a district-owned computer or through the district's technology.

Students are not permitted to access any rating or dating websites from the district's technology.

Do not access material that is offensive, profane, or obscene including pornography and hate literature. Hate literature is anything written with the intention to degrade, intimidate, incite violence, or incite prejudicial action against an individual or a group based on race, ethnicity, nationality, gender, gender identity, age, religion, sexual orientation, disability, language, political views, socioeconomic class, occupation, or appearance (such as height, weight, and hair color).

Communication: Instant Messaging, E-mail, Posting, Blogs

Students are not permitted to access from the district's technology any instant messenger services.

Inappropriate communication is prohibited in any public messages, private messages, and material posted

online by students. Inappropriate communication includes, but is not limited to the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by students; information that could cause damage to an individual or the district community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If you are told by another person to stop sending communications, you must stop.

Students may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. This is unacceptable student behavior known as cyber-bullying and will not be tolerated. Any cyber-bullying, on or off-campus, that is determined to substantially disrupt the safety and/or well-being of the district is subject to disciplinary action.

Intellectual Property, Academy Honesty, Personal Integrity and Plagiarism

Do not claim or imply that someone else's work, image, text, music, or video is your own. This is plagiarism and will not be tolerated. Plagiarism is also when you incorporate a piece of someone else's work into your own without giving them appropriate credit. All students are expected to maintain academic honesty. Do not pretend to be someone else online or use someone else's identity. Do not use, post, or make accessible to others the intellectual property; including, but not limited to text, photographs, and video; of someone other than yourself. This includes intellectual property that you were given permission to use personally, but not publically. This behavior violates district policy as well as state and federal laws.

A work or item is copyrighted when, among other issues, one person or one group owns the exclusive right to reproduce the work or item. Songs, videos, pictures, images, and documents can all be copyrighted. Copyright infringement is when you violate copyright law and use or reproduce something

without the authority to do so. Make sure to appropriately cite all materials used in your work. Do not utilize some else's work without proper permission.

Data and Gaming Devices

Students are allowed to bring their personal iPods, MP3 players, CD players, DVD players, or other similar data-accessing devices onto campus, but are not allowed to utilize these devices during academic hours without staff permission.

Students are not allowed to bring personal video game systems onto campus or to district events without specific prior permission from school personnel.

Students may not use district-owned computers to play computer games unless they are approved as educational curricular materials.

Downloads and File Sharing

Students may never download, add, or install new programs, software, or hardware onto district-owned computers. Downloading sound and video files onto district-owned computers is also prohibited. This prohibition applies even if the download is saved to a removable hard drive.

Students may never configure their district computer or personally owned computer to engage in illegal file sharing. The district will cooperate fully with the appropriate authorities should illegal behavior be conducted by students.

The likelihood of accidentally downloading a virus or spyware when downloading music and movies is very high; therefore students may not download any sound or video files onto their personally-owned technological devices through the district's technology. Students may not download any computer game files or attachments from unknown senders.

Commercial and Political Use

Commercial use of district technology is prohibited. Students may not use district technology to sell, purchase, or barter any products or services. The district is not responsible for any damages, injuries, and/or claims resulting from violations of responsible use of technology. Students who are engaged in fund-raising campaigns for district sponsored events and

causes must seek prior written approval from district administration before using technology resources to solicit funds for their event.

Political use of district technology is prohibited without prior, specific permission from a district administrator or advisor. Students may not use district technology to campaign for/against, fundraise for, endorse, support, criticize or otherwise be involved with political candidates, campaigns or causes.

Respect for the Privacy of Others and Personal Safety

Our district is a community and as such, community members must respect the privacy of others. Do not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to others. Do not misrepresent or assume the identity of others. Do not re-post information that was sent to you privately without the permission of the person who sent you the information. Do not post private information about another person. Do not use another person's account. If you have been given an account with special privileges, do not use that account outside of the terms with which you were given access to that account.

Do not voluntarily post private information about yourself online, including your name, your age, your school name, your address, your phone number, or other identifying information.

Computer Settings and Computer Labs

Students are not permitted to alter, change, modify, repair, or reconfigure settings on any technology device with the intent to hide unacceptable or illegal use of their own devices. This includes deleting cookies and history and re-setting the time and/or date on the computer.

Purposefully spreading or facilitating the spread of a computer virus or other harmful computer program is prohibited.

Food and drink are prohibited from district computer labs. Students may not eat or drink while using any district-owned computers or other technologies.

Students may not circumvent any system security measures. The use of websites to tunnel around firewalls and filtering software is expressly

	prohibited. The use of websites to anonymize (hide identity) the user are also prohibited. The use of websites, both domestic and international, to circumvent any district policy is prohibited. Students may not alter the settings on a computer in such a way that the virus protection software would be disabled. Students are not to try to guess passwords. Students may not simultaneously log in to more than one computer with one account. Students are not to access any secured files, resources, or administrative areas of the district network.	1 2 3 4 5 6 7 8 9 10 11 12 13
Response Section	The district's administrators shall have broad authority to interpret and apply these policies. Violators of our technology policies will be provided with notice and opportunity to be heard in the manner set forth in the District Handbook, unless an issue is so severe that notice is either not possible or not prudent in the determination of the school administrators. Restrictions may be placed on violator's use of district technologies and privileges related to technology use may be revoked entirely pending any hearing to protect the safety and well-being of our community. Violations may also be subject to discipline of other kinds within the district's discretion. Our district cooperates fully with local, state, and/or federal officials in any investigations related to illegal activities conducted on district property or through district technologies. District authorities have the right to confiscate personally-owned technological devices that are in violation or used in violation of district policies. If you accidentally access inappropriate information or if someone sends you inappropriate information, you should immediately tell a teacher, administrator or a member of the Technology Services Department so as to prove that you did not deliberately access inappropriate information. If you witness someone else either deliberately or accidentally access inappropriate information or use technology in a way that violates this policy, you must report the incident to an administrator as soon as possible. Failure to do so could result in disciplinary action. The district retains the right to suspend service, accounts, and access to data, including student files and any other stored data, without notice to the student if it is deemed that a threat exists to the integrity of the district network or other safety	14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53

	concern of the district.	1 2 3 4
District Liability	The district cannot and does not guarantee that the functions and services provided by and through our technology will be problem free. The district is not responsible for any damages students may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or the quality of the information obtained through district technologies. Although the district filters content obtained through district technologies, the district is not responsible for student's exposure to "unacceptable" information nor is the district responsible for misinformation. The district is not responsible for financial obligations arising through the use of district technologies.	5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
General Safety and Security Tips for the use of Technology	The district will 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. Never post personal information about yourself online. Personal information includes your phone number, address, full name, siblings' names, and parents' names. When creating an account on a social networking website, make sure to set your privacy settings so only your friends can view your pictures and your profile. Avoid accepting a friend you do not already know. If possible, set up your account so that you are notified of any postings onto your wall or page. If possible, set up your account so that you have to approve all postings to your wall or page. If possible, set up your account to notify you when someone else has posted and tagged you in a picture. If you have a public profile, be careful about posting anything identifiable such as a sports team number or local park where you spend your free time. Think before you send all forms of communication, including emails, IM's, and text messages. Once you send the data it is not retrievable, and those who receive it may make it public or send it along to others, despite your intentions. Do not feel bad about ignoring instant messages or e-mails from unknown people. Save all contacts from known or unknown people who are repeatedly contacting or harassing you. These saved messages will help authorities track, locate, and prosecute cyber-	22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53

stalkers and cyber-bullies. If you have been speaking with a stranger online and make plans to meet the stranger in person, notify your parents or guardians first.

Do not share your passwords with your friends. When creating a password, do not make it anything obvious such as your pet's name or favorite sports team. Also remember to include both letters and numbers in your password if possible.

Do not open or run files on your computer from unknown or suspect senders and sources. Many viruses and other undesirable consequences can result from opening these items.

Do protect your own computer and devices by keeping antivirus and antispyware up to date. Keep your operating system and application software up to date. Turn off file sharing as an option on your computer.