

SECTION: OPERATIONS

TITLE: Staff Internet, E-Mail
and Network Resources
Access Agreement

ADOPTED:

REVISED: July 18, 2011
May 21, 2012

Lebanon School District

Introduction and Overview	<p>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.</p> <p>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.</p> <p>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</p>	<p>1 2 3 4 5 6 7 8 9 10 11 12 13 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</p>
---------------------------	---	--

	assistance.	1
		2
Supervision	All adults utilizing our school buildings and our	3
and Personal	technology are also subject to the terms and	4
Responsibilit	conditions of this Technology Use Policy.	5
y		6
	All employees must sign an agreement stating that	7
	he/she has read and agrees to the terms and conditions	8
	in the technology policy before they can utilize any	9
	district technologies. This permission form must be	10
	signed one time only for new hires unless the form is	11
	updated in a subsequent year. All signed	12
	acknowledgements will be kept on file in the Human	13
	Resource Department.	14
		15
	District employees may use the district technology in	16
	the course of their regular job responsibilities.	17
	Incidental personal use is permitted as long as it	18
	does not interfere with job performance or the	19
	district's operation of information technologies,	20
	financially burden the district or otherwise violate	21
	district polices or state and federal laws. It is	22
	important that employees who are working with students	23
	(teachers, paraprofessionals, counselors, etc.) need	24
	to be aware of the following: During instructional	25
	time, the personal use of technology is not permitted	26
	and must be silenced.	27
		28
		29
Privacy	The district reserves the right to monitor and track	30
	all behaviors and interactions that take place on	31
	district owned equipment. We also reserve the right	32
	to investigate any reports of inappropriate actions	33
	related to any technology used at school. All e-mails	34
	and messages sent through the district's network or	35
	accessed on a district computer can be inspected. Any	36
	files saved onto a district computer can also be	37
	inspected. Employees have a limited expectation of	38
	privacy when using their own technology on district	39
	property or at district events so long as no activity	40
	violates policy, law and/or compromises the safety and	41
	well-being of the district community.	42
		43
		44
		45
Filtering	Our district adheres to the requirements set forth by	46
	the United States Congress in the Children's Internet	47
	Protection Act. This means that all access to the	48
	Internet is filtered and monitored. The district	49
	cannot monitor every activity, but retains the right	50
	to monitor activities that utilize district owned	51
	technology. By filtering Internet access, we intend	52
	to block offensive, obscene, and inappropriate images.	53

Right to Update	Since technology is continually evolving, our district reserves the right-to-change, update, and edit its technology policies at any time in order to continually protect the safety and well-being of our district's community. To this end, the district may add additional rules, restrictions, and guidelines at any time.	1 2 3 4 5 6 7 8 9 10 11
Termination of Accounts and Access	Upon termination of your employment within our district, you will no longer have access to the district network, files stored on the district network, or your district-provided email account. We recommend saving all personal data stored on district technology to a removable hard drive periodically throughout your employment. If you leave our institution in good standing, such as by reason of retirement, we will provide you with email forwarding for a period of 60 days after your termination date.	12 13 14 15 16 17 18 19 20 21 22
Definitions and Terms Section	<p>Bandwidth is a measure of the amount of data that can be transmitted in a fixed amount of time.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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,</p>	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

	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 operated by the district.	1 2 3 4 5 6 7 8
	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 faculty members, staff members, parents, and any visitors to the campus.	9 10 11 12 13 14 15
	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.	16 17 18 19 20
	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.	21 22 23 24 25 26
Acceptable Uses Section	User Orientation	27 28
	All new employees must attend a professional development induction that includes reviewing acceptable and unacceptable behaviors related to technology before they can utilize any district technologies. This session is only required once.	29 30 31 32 33 34
	Purposes and Use Expectations for Technology	35 36
	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, and limited high quality self-discovery activities. Commercial and recreational use of district technology resources is prohibited. Employees may not utilize district technology to sell, purchase, or barter any products or services. The district is not responsible for any damages, injuries, and claims resulting from violations of responsible use of technology.	37 38 39 40 41 42 43 44 45 46 47 48 49
	Personal Responsibility	50 51
	We expect our employees to act responsibly and thoughtfully when it comes to using technology.	52 53

Technology is a finite, shared resource offered by the district to its employees and students for academic pursuits. Employees bear the burden of responsibility to inquire with the Technology Services Department or other district administrators when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

District Provided Technology Resources

Network storage is a finite district resource and we expect employees to be respectful of other users and limit the amount of space and memory taken up on district computers and on the district network.

All designated employees (administrators, teachers, secretaries and technology staff) are provided with a district e-mail account. All e-mails sent from this account are representative of the district and employees should keep in mind district policies regarding appropriate language use, harassment, defamation, and other policies and laws. Employee e-mail accounts are subject to monitoring and have limited privacy. Employees are sharing resources such as bandwidth and server space with others and downloading large files utilizes finite resources. Abusing these resources can result in the loss of this privilege. Please delete old e-mails and save large attachments elsewhere to limit the amount of storage space your e-mail account is using.

This district has wireless network that is password protected. If you desire to connect your laptop or hand held device to the network, you must contact a member of the Technology Services Department. Unauthorized access is forbidden.

The district provides individual technology accounts for designated employees. Users must log off when they are finished using a district computer. Failing to log off may allow others to use your account, and employees are responsible for any activity that occurs through their personal account. An employee is responsible for the use of his/her technology account, including students, children, and/or spouses.

The district provides technologies for educational use. The district reserves the right to collect district owned hardware periodically to do routine maintenance and for safe keeping during summer and/or extended breaks. Teachers that are on extended leave will be expected to turn in their technology to the Technology Services Department.

<p>Unacceptable Uses of Technology Section</p>	<p>Mobile Devices</p> <p>Cell phones, smart phones and PDA's are permitted on campus, but are not to be used during class time except for district related emergencies. Instant messaging, phones, and other distracting noises from personal devices must be silenced during instructional time.</p> <p>Social Networking and Website Usage</p> <p>Employees may have social networking profiles or accounts, but these profiles/accounts may not be accessed during instructional time from either personally owned or district owned technology. In addition, teachers and staff should not communicate with students or parents/guardians through these profiles/accounts.</p> <p>Employees are not permitted to access any photography sharing websites from a district-owned computer or through the district's technology.</p> <p>Employees are not permitted to access any rating or dating websites from the district's technology.</p> <p>Employees shall 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).</p> <p>Communication: Instant Messaging, E-mail, Posting, Blogs</p> <p>Inappropriate communication is prohibited in any public messages, private messages, and material posted online by employees. 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 employees; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment</p>	<p>1 2 3 4 5 6 7 8 9 10 11 12 13 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</p>
--	--	--

(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.

Employees may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy their colleagues or others in our community. This is unacceptable behavior and will not be tolerated. Any behavior, on or off-campus, that is determined to substantially disrupt the safety and/or well-being of the school is subject to disciplinary action.

Do not post or send chain letters or spam. Spamming is sending an unnecessary and unsolicited message to a large group of people. Spamming can occur through e-mails, instant messages, or text messages.

Please contact the Human Resource Department if you believe you are a victim.

Downloads and File Sharing

Employees may never download, add, or install new programs, software, or hardware onto district-owned computers.

Employees 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 employees.

Employees also should not download any files or attachments from unknown senders.

Commercial and Political Use

Commercial use of district technology is prohibited. Employees 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. Employees who are engaged in fund-raising campaigns for district sponsored events and causes must seek prior written approval from your supervisor before using technology resources to solicit funds for their event.

	Respect for the Privacy of Others and Personal Safety	1
		2
		3
	Our district is a community and as such, community	4
	members must respect the privacy of others. Do not	5
	intentionally seek information on, obtain copies of,	6
	or modify files, other data, or passwords belonging to	7
	others. Do not misrepresent or assume the identity of	8
	others. Do not re-post information that was sent to	9
	you privately without the permission of the person who	10
	sent you the information. Do not post private	11
	information about another person. Do not use another	12
	person's account. If you have been given an account	13
	with special privileges, do not use that account	14
	outside of the terms with which you were given access	15
	to that account.	16
		17
	Be careful when posting private information about	18
	yourself online, including your name, your address,	19
	your phone number, or other identifying information.	20
		21
	Computer Settings	22
		23
	Employees may not circumvent any system security	24
	measures. The use of websites to tunnel around	25
	firewalls and filtering software is expressly	26
	prohibited. The use of websites to anonymize (hide	27
	identity) the user are also prohibited. The use of	28
	websites, both domestic and international, to	29
	circumvent any district policy is prohibited.	30
	Employees may not alter the settings on a computer in	31
	such a way that the virus protection software would be	32
	disabled. Employees are not to try to guess	33
	passwords. Employees may not simultaneously log in to	34
	more than one computer with one account. Employees	35
	are not to access any secured files, resources, or	36
	administrative areas of the district network without	37
	express permission or the proper authority.	38
		39
		40
Response	The district's administrators shall have broad	41
Section	authority to interpret and apply these policies.	42
	Violators of our technology policies will be provided	43
	with notice and opportunity to be heard in the manner	44
	set forth in the Employee Handbook, unless an issue is	45
	so severe that notice is either not possible or not	46
	prudent in the determination of the district	47
	administrators. All violations will be reported to	48
	the immediate supervisor and the head of the Human	49
	Resource Department. Restrictions may be placed on	50
	violator's use of district technologies and privileges	51
	related to technology use may be revoked entirely	52
	pending any hearing to protect the safety and well-	53

	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.	1 2 3 4 5 6 7 8 9 10
	If you accidentally access inappropriate information or if someone sends you inappropriate information, you should immediately tell a supervisor, administrator, or a member of the Technology Services Department so as to prove that you did not deliberately access inappropriate information.	11 12 13 14 15 16 17
	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 a supervisor or administrator as soon as possible. Failure to do so could result in disciplinary action.	18 19 20 21 22 23 24
	The district retains the right to suspend service, accounts, and access to data, including employee files and any other stored data, without notice to the employee if it is deemed that a threat exists to the integrity of the district network or other safety concern of the district.	25 26 27 28 29 30 31 32
Technology 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 cannot guarantee the functionality of district owned hardware and/or network operations. The district is not responsible for any damages employees 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 an employee'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.	33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
General Safety and	Posting Online and Social Networking: Be careful when posting personal information about yourself online.	51 52 53

Security Tips
for the use
of Technology

Personal information includes your phone number, address, full name, and other similar information. Remember that anyone might see what you post.

Communications: Think before you send all forms of communication, including emails, 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.

Strangers: 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-stalkers.

Passwords: Do not share your passwords with others. 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.

Downloads and Attachments: 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.

1
2
3
4
5
6
7
8
9
10
11
12
13
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