No.815

SECTION: OPERATIONS

TITLE: Social Media Employee Risk Policy

ADOPTED: July 18, 2011

REVISED:

Lebanon School District

Introduction and Overview	The Lebanon School District gives you access to Social Media to perpetuate business only. You are WARNED that sending business electronic messages from Lebanon School District's work servers or remote locations (including but not limited to your home, friend's house, Wi-Fi, and other public places) connecting to the district's server is risky and privacy cannot be guaranteed. You should always develop electronic content with the understanding that your message may be intercepted by a stranger and could be used against you in court or internally. Despite having industry grade computer privacy protection software and hardware, your personal social media posts and e-mails could be hacked. Also, during an internal administrative disciplinary proceeding or legal claim, your personal electronic messages could be used against you. (See (Electronic Communications Privacy Act of 1986 (ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510), E-discovery Amendments to the Federal Rules of Civil Procedure, December 1, 2006), Therefore, your use of the Lebanon School District server and all equipment from work or from remote locations is a privilege and contingent on satisfying the following conditions: 1) You affirm that you read the entire document-word for word; 2) You understand the risks cited in this policy and agree that there may be hidden legal risks that Lebanon School District can not reasonably anticipate and therefore are not listed; 3) If you have questions about the risks and other terms cited in the policy, you agree to put them in writing and send them by letter or e-mail to the Technology Services Department no later than five business days after signing the consent form on the bottom of this policy;

	4) YOU AGREE THAT IF YOU VIOLATE THIS RISK POLICY, YOU WILL BE EXPOSED TO PENALTIES UNDER THE LEBANON SCHOOL DISTRICT'S ADMINISTRATIVE REGULATIONS, CIVIL LAW, CRIMINAL LAW, AND COMMON LAW. YOU ALSO AGREE THAT BY SIGNING THIS DOCUMENT YOU AGREE THAT YOU HAVE BEEN ADEQUATELY WARNED ABOUT THE REASONABLY ANTICIPATED SOCIAL MEDIA AND E-MAIL RISKS AND YOUR FAILURE TO SATISFY THE STATED CONDITIONS ABOVE COULD NOT BE DIRECTLY OR INDIRECTLY CAUSED BY CLAIMING YOU DIDN'T UNDERSTAND THIS SOCIAL MEDIA RISK POLICY. YOU AGREE THAT YOU WERE GIVEN A REASONABLE OPPORTUNITY TO ASK QUESTIIONS AND CLARIFY ANY CONFUSION YOU MAY HAVE HAD ON ANY PART OF THIS POLICY. THEREFORE, YOU AGREE THAT LEBANON SCHOOL DISTRICT ACTED IN A REASONABLE MANNER IN EXPLAINING THIS ELECTRONIC MAIL AND SOCIAL MEDIA POLICY TO YOU. YOU AGREE THAT IF YOU FILE A FAILURE TO NOTIFY OR TRAIN CLAIM UNDER 42 USCS 1983 REGARDING LEBANON SCHOOL DISTRICT'S SOCIAL MEDIA AND E-MAIL POLICY, IT WOULD BE A BASELESS CLAIM AND YOU AGREE TO INDEMNIFY AND HOLD HARMLES LEBANON SCHOOL DISTRICT FOR ANY ABUSE OF THIS POLICY OR OTHER COMPUTER AND INTERNET RELATED POLICIES.
The Inherent Risks Using Social Media	The Lebanon School District seeks to support employees in their BUSINESS use of the district's computer server and equipment in using all social media. It is the district's ultimate goal to assist the user in balancing the risks listed below with using social media in a productive manner. Sending social media posts and e-mails (i.e. Facebook, Blogs) have inherent risks: • Despite using industry standard privacy strategies, your data may be hacked; • Your messages can be forwarded and rewritten to unauthorized receivers; • Your social media posts could be used years later in a legal claim; • Your use of a personal social media accounts at work doesn't always guarantee privacy; • You can destroy a person's reputation instantaneously and permanently with one message; • You can invade a person's privacy by revealing health or other private facts; • Your opinions may be not be protected speech under the First Amendment; • Your opinions may be considered facts not opinions in court; • Your words, pictures and audio may violate state and federal civil and criminal laws;

New Risks Of Creating Public Records On Your Own Internet Connection	• Your messages could violate Pennsylvania's public record laws (F.S. 119); • Your messages may be used as admissions. (Federal and State Hearsay Exceptions); • Your messages may be used as excited utterances in court. (Federal and State Hearsay Exceptions); • Your messages may be used as proof of a person's mental or physical state in court. (*Hearsay exceptions; availability of declarant immaterial, Federal Rules 803*) (*See Chaplinsky v. New Hampshire, 315 U.S. 568 (1942)*, (*See Black's Law Dictionary Defining Negligence*) All employees must recognize that there is a higher duty of care in using social media. Employees must only develop content that reflects their scope of expertise and send messages only to authorized receivers. Courts do not accept defenses of ignorance of the law or claiming it was an innocent mistake. Courts no longer offer immediate privacy protection at work or at a remote location using portable media. All social media content must be created with sensitivity to local, state, and federal laws. When you send job related decision-making electronic messages on your own personal social media or portable media accounts or someone else's Internet connection (i.e. using a connection not sanctioned by your organization) you are considered the custodian of those records. Thus, you are responsible for safeguarding the records and making them available for inspection. You realize the social network company my have a different terms of service on retrieving records which could conflict with your state's public record laws. Additionally, you understand that by creating these records, you have an affirmative obligation to inform your supervisor or appropriate person (i.e. attorney, technology director, others). You understand that records created on your own Internet connection may constitute a public record under your state and Federal public records laws. Therefore, you must maintain the integrity of the record and make it accessible for public inspection according to your public record guidelines. Based on this knowledge, you affirm that you have been appropriately informed of the risks in creating public records on non-employer sanctioned Internet connections and personal equipment (including, but not limited to your store-bought portable phones,

Fundamental Causes Of Action Leading To Social Media Liability	electronic devices of friends or relatives, and home computers). Upon signing this agreement, you affirm that you have been informed and clearly understand that private social media sites such as Facebook, MySpace, Linkin, YouTube and other sites may not be bound by specific state and Federal public records. Therefore, you understand that you are taking a major risk by using these sites in any way to comment on public issues or job related activities that could be considered public records open to public inspection. Finally, by signing this document you have been reasonably informed and clearly understand that commenting on social media sites and blogs about public issues or job related activities could be a violation of your public record exemptions exposing you to professional and personal liability. In developing these types of public records you agree to do the following: • Notify the appropriate authority that a public record has been created. • Specify where the record was can be found. • Specify the social media site or other location you used to send or receive records Your causes of action in sending electronic mail are not limited to but may include: 1) **Libel Claims:** Sending or forwarding false electronic mail statements or true statements with malice can trigger libel claims. Libel can occur when you disparage a person's reputation and lower their self-esteem in the community. All employees must be aware of a shift by some courts regarding truth as absolute defense to libel. Some courts have ruled that the truth is not always a defense to libel where actual malice is proven. *(See Alan S. Noonan v. Staples Inc., No. 07-2159, (U.S. Court Of Appeals 1st Circuit, MA February 13, 2009)* 2) **Privacy Claims:** Sending or forwarding private facts can trigger invasion of privacy claims. 3) **Criminal Claims:** Sending or forwarding threats of bodily harm and death can trigger federal and state criminal penalties *See United States v. DeAndino, 958 F.2d 146 (US Ct. App. 6th Cir. 1992)* 4) **Copyright Claims:** Sending or forwarding

Categories Of Opinions Not Always Protected By The First Amendment	copyrighted material can trigger federal copyright violations *(See Article I, Section 8, Clause 8).* 5) **Health Privacy Claims:** Sending or forwarding private health or financial information can trigger state and federal penalties *(See Health Insurance Portability and Accountability Act (HIPAA) Public Law 104-191,1996, Privacy Rules 45 CFR Part 160 and Subparts A and E of Part 164. and Sarbanes-Oxley Act of2002(Pub.L. 107-204, 116 Stat. 745, enacted July 30)*
Fundamental Electronic Mail Privacy Issues	It is settled law that the following types of speech may not be covered under the First Amendment and could expose you to liability when you send e-mail or post statements on Facebook, Twitter, Blogs or other social media *(Source: Chaplinsky v. New Hampshire, 315 U.S. 568 (1942):* • Defamatory Speech: E-mails or social media opinions that defame are NOT protected speech. • Hate Speech: Hateful opinions are NOT always protected speech. • Inciting Speech: Opinions that may incite a riot or harm are NOT always protected speech. • Offensive Speech: Opinions that have no literary, scientific, or artistic value are NOT always protected speech. *See Miller v. California, 413 U.S. 15 (1973)* All of Lebanon School District's employees using the employer's server or gaining access to the server from remote devices on their own personal Internet connection, are hereby notified that their content may be monitored by Lebanon School District. The employer reserves the right by federal and state law to properly maintain the integrity of our electronic communications system. Although the Lebanon School District uses industry standard encryption tools and privacy practices, it is impossible to guarantee an employee's data could never be stolen or misused. These are always inherent risks of computer hacking when employees send a personal or business e-mail or uses Facebook, and other social media. (See Electronic Communications Privacy Act of 1986 (ECPA Pub. L. 99-508, Oct. 21, 1986). Employees must also be aware that the following behavior can expose you to violations of state and federal privacy laws: • Sending or forwarding unauthorized health information-this ranges from sending a casual e-mail about another person's health to collecting

Distinguishing Between Personal and Business Electronic Messages	money for a sick co-employee. *(See HIPAA cite above)* • Sending or forwarding unauthorized financial information-this ranges from sending an opinion on the bankruptcy of another employee to revealing their stock portfolio. *(See Katz v. United States, 389 U.S. 347 (1967)* In legally determining whether your electronic messages are transitory or business, there is usually a two-part test. The first part of the test involves a determination if your electronic message is a public record under your state laws or it's considered a business document. If your message does not qualify as a public record, the step is to determine whether the content of the message deserves privacy protection according to public policy. This determination depends on your state and federal laws. You are advised that just because the message is personally embarrassing to you doesn't mean the law will consider your message worthy of privacy protection. Additionally, you are hereby informed that your liability is NOT based on whether you sent your message from a personal e-mail box or what device and location you transmitted from. Your liability is judged on the content of your message. Therefore, the following messages may not be considered personal: • A message that contains your personal opinion on a public issue using social media. • A message that contains your personal opinion on a public issue using your cell phone. • A message that contains your personal opinion on a public issue using a blog. • A message that contains your personal opinion on a public issue using any Web 2.0 platform. • A message that contains your personal opinion on a public issue using your personal website. • A message that contains your personal opinion on a public issue using your home computer. • A message that contains your personal opinion on a public issue using your personal laptop.
Announcing The Liability Risks Of Using Social Media	• A message that contains your personal opinion on a public issue using private Internet accounts. • A message that contains your personal opinion on a public issue using WiFi at a remote location. • A message that is sent to a co-worker and contains both personal and public facts. • A message that is sent to a private citizen concerning public business.

All employees are on formal notice that by using social media you are mass communicating to a potential audience of millions of people. This elevates your duty of care as follows:

1) You have a higher duty of care in sending messages only to authorized receivers.
2) You have a higher duty of care to avoid sending public records that exclude others (i.e. Friends List).
3) You have a higher duty of care sending messages that are business related.
4) You have a higher duty of care sending messages that are health related. (See HIPAA Laws)
5) You have a higher duty of care sending messages that related to finances.
6) You have a higher duty of care sending messages regarding promotions or disciplinary procedures.
7) You have a higher duty of care to report all offensive and threatening messages to your superiors.
8) You have a higher duty of care to avoid retaliating against offensive and threatening messages.
9) You have a higher duty of care and are bound by federal law to avoid deceptive subject lines.
10) You have a higher duty of care to create subject lines that comport with the body of the message.
11) You have a higher duty of care to avoid blank subject lines.
12) You have a higher duty of care to avoid using Blind Carbon Copies unless authorized by your superiors.
13) You have a higher duty of care to develop electronic content that reflects your scope of expertise.
14) You have a higher duty of care to develop electronic content that is professionally written.
15) You have a higher duty of care to avoid jokes, offensive symbols, abbreviations and other risky speech.
16) You have a higher duty of care to avoid statements that reveal a person's private health information.
17) You have a higher duty of care to avoid statements that reveal a person's private financial information.
18) You have a higher duty of care to avoid offering legal or medical advice without a state license.
19) You have a higher duty of care to avoid accusing a person of a crime.
20) You have a higher duty of care to avoid accusing

	a person of sexual promiscuity. 21) You have a higher duty of care to avoid accusing a person of having bad character. 22) You have a higher duty of care to avoid accusing someone of being mentally or physically defective. 23) You have a higher duty of care to avoid libelous or offensive audio, video and other attachments. 24) You have a higher duty of care to avoid forwarding messages to unauthorized receivers. 25) You have a higher duty of care to review all e-mail messages prior to forwarding. 26) You have a higher duty of care to understand that forwarding offensive content exposes you to liability. 27) You have a higher duty of care to immediately forward child pornography your superiors. 28) You have a higher duty of care to report messages containing threats of bodily harm or property damage. 29) You have a higher duty of care to avoid deleting any public records unless authorized by your superiors. 30) You have a higher duty of care to avoid deleting e-mails or other records when there is a litigation hold. 31) You have a higher duty of care to avoid deleting any e-mails during an internal investigation. 32) You have a higher duty of care when you knew or should have known there is an internal investigation. 33) You have a higher duty of care to provide your full name, address, and phone number in all e-mails. 34) You have a higher duty of care to avoid using the employer's computer equipment for private business. 35) You have a higher duty of care to avoid promoting or marketing your private business with Lebanon School District computer equipment (i.e. sending out mass e-mails that violate the **CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108-187.**	
Announcing The Liability Risks Of Using Social Media	Social Media includes but is not limited to social networking platforms such as Facebook, Twitter, LinkedIn, and other collaborative sites, mobile phones, interpersonal sites such as WebEx, podcasts, photo-sharing sites, publishing websites, audio and video websites such as YouTube, Wikipedia, search engines, virtual worlds, gaming, livecasting, productivity applications, Rich Site Summary tools,	

and other interactive platforms designed for users to collaborate. These and other social media platforms are NOT insulated from civil and criminal laws. Despite any claims made by Internet providers or website owners that you have the First Amendment right to express your opinions, all employees are on notice that posting on-line opinions are subject to libel and invasion of privacy claims. Further the court may find your opinions are actually statement of facts that can be proven true or false by a jury. (See *Milkovich v. Lorain Journal Co.*, 497 U.S. 1 (1990). Also, due to the weak nature of the Internet, notwithstanding privacy promises, no social network can reasonably guarantee you privacy protection. Based on the announcement of these inherent risks, you agree to always verify with the city attorney, or other designated superior before posting or sending any opinions on work related issues or others social media posts that could be linked to the perpetuation of district business. You are hereby made aware that you have a higher duty of care in using social media as public employees and elected officials. You are also on notice that using the defense in court, "that you were acting as a private person" will not protect you. Upon signing this policy, you clearly understand the terms below and agree to do the following:

1) Only use social media platforms to post generic public record notices (no commentary).
2) Always check with your attorney or superiors before posting opinions on public records.
3) Recognize that your opinions on social media may violate your public record exemptions.
4) Recognize that all your business comments on social media are valid state public records.
5) Recognize that employees have a higher duty of care in writing messages.
6) Recognize that violation of civil and criminal laws could expose you to personal liability.
7) Refrain from using your official title when using social media to discuss personal issues.
8) Refrain from modifying a public record with opinions on social media platforms.
9) Refrain from posting offensive, negligent, or criminal statements on social media.
10) Refrain from forwarding possible libelous jokes or opinions on social media.
11) Refrain from using the city server to create anonymous posts.
12) Refrain from falsifying your identification when collaborating on social media.
13) Refrain from uploading or downloading offensive audio and video on all social mediums.
14) Refrain from engaging in all civil or criminal

Announcing The Liability Risks Of Home Computers and Portable Media	violations on all social mediums. 15) Recognize that all statements on social media are exposed to libel and privacy claims. 16) Recognize that Internet Providers have special laws that can protect them from liability. 17) Recognize that all audio, video, and pictures can be hacked and misused on social media. 18) Recognize that social media gives out your profiles to advertisers on social media 19) Agree that you will not transmit confidential district information on any social networks. 20) Agree that you will not mix business content with personal posts on social media. 21) Agree that you will not send libelous or offensive statements to others on-line. 22) Agree that you will not share unauthorized private facts of others on social media. 21) Agree that you will not engage in unauthorized commercial e-mail with venders on-line.
Policy Modification Prohibition	Employees are now on notice that due to advancement in portable media technology, you have little or no expectation of privacy at home regarding the creation and storing of public record documents. Courts recognize that new portable technologies have empowered employees to work at home or in other remote locations. Additionally, the 2006 amendments to the Federal Discovery Laws expanded the power of attorneys to search for relevant evidence in home computers and portable media. Courts base their decisions on relevant content, not where it is was stored or whether you purchased the equipment with your money. All employees agree that upon reading this policy you possess the following knowledge; • You know that social media companies <u>can not guarantee</u> privacy or insulate you from lawsuits; • You know that blog or website owners <u>can not guarantee</u> privacy or insulate you from lawsuits; • You know that offering your opinions as public employees on social media is risky; • You know that all social media users are exposed to liability for unprotected speech; • You know that you may face personal liability because your statements are facts not opinions; • You know that statements on social media sites can permanently damage a person's reputation; • You know that Internet providers are insulated from liability under various federal laws; **NO EMPLOYEE OR THIRD PARTY VENDOR IS AUTHORIZED TO MODIFY THIS AGREEMENT IN PART OR WHOLE VERBALLY OR IN**

	WRITING. ALL MODIFICATIONS MUST BE MADE BY THE ORGANIZATION'S ATTORNEY OR AUTHORIZED PERSON.