

School Board of Levy County

E-MAIL AND Computer Use POLICY

Policy:

The computer system in your office, classroom, or other area is the property of the School Board of Levy County (SBLC) and is intended to be used for approved educational purposes only. You have no expectation of privacy with our governmental computers on site. You have no expectation of privacy accessing our server from off-site locations.

There is no personal use of the computer including but not limited to the following activities: 1) e-mail communication that contains in the body of the e-mail message itself or attachment content that can be construed in nature as terrorist, racial, sexual, ethnic, gender, or age offensive; 2) personal financial information transmitted through text or pictorial attachments; 3) taking your computer off the filtering proxy or attempting to bypass the proxy set up to be in compliance with the Child Internet Protection Act; 4) attempting to hack into servers or systems located within our local area network (LAN), wide area network (WAN), or off site locations; 5) installing or loading software on a SBLC computer without proper approval. Any questions on whether a message or Internet site qualifies as reasonable business purpose should be directed to the human resources department before going on-line.

Comments/Procedures:

1) *No Expectation of Privacy:* As providers of the computer equipment and servers. Federal and State laws give us the right to monitor your business communications on our computers. This statutory authority is based on ensuring the appropriateness of business communications, random computer system checks and actual and implied consent by the user's written acknowledgment of clearly understanding this policy. The act of signing this document signifies the user clearly understands the policy and agrees to execute this policy in good faith. Additionally, the user waives any privacy rights or claims of inadequate training (42 USCS 1983 & 27), that SBLC showed a deliberate indifference in properly training the user on the proper use of the computer at work.

2) *Public Records:* The user of SBLC computers recognizes they are bound by state public record laws, and documents that are created to formalize knowledge or transact business of SBLC are considered public record and are open to the review and copying of the general public. This includes all work records on your computer system, data transmitted over our server from on site or off-site locations and portable media such as disks, floppy disks, CD's and any other transportable media. All records must be retained according to Chapter 119 of the Florida Public Records Statute.

Prohibited Activities

General Prohibitions: There absolutely can be no creation, downloading from another web site, linkage to another web site, transmittal from your computer to a co-worker computer or outside computer information that is: 1) harassing; 2) defamatory; 3) discriminatory; 4) profane; 5) violates federal copyright, and trademark law and federal or state trade secret laws, or violates other federal and state civil or criminal statutes. It is incumbent upon the computer user of SBLC computer equipment to familiarize themselves with the basics of what specific communication triggers sexual harassment, other harassment, copyright, trademark and other relevant computer abuse laws. If a computer user has an uncertainty whether their behavior could violate a federal or state statute, they have an affirmative obligation to contact their in-house attorney or human resources department before using the computer.

Lack of knowledge is not a defense to computer abuse or violation of laws. Computer user waives all defenses that they were inadequately trained or not clearly warned about the necessity of being educated on all federal and state laws regarding computer abuse and criminal activity. Upon signing an acknowledgment of clearly understanding this policy agreement, the computer user recognizes a higher duty of care in using the computer because text based messages, pictures, audio and video, and documents can reach a large audience within seconds.

Waste of Computer Resources: Computer users understand there are Federal and State laws prohibiting Spam mail—unsolicited mail or mass mail—or chain letters. The computer user will not monopolize Internet access or negatively affect the bandwidth in any manner that transcends normal computer use (ie: actions by you or students which consist of downloading MP3's, listening to radio programs, or watching TV broadcasts in the classroom except as used as part of the regular instructional program of a school).

E-Mail Myths: Computer users understand that based on the architecture of the Internet or Intranet, their e-mail and attachments may cross other servers before the intended receiver receives the correspondence. This means the user realizes their message or attachment may be intercepted and the security of e-mail or the Internet is vulnerable. Therefore, sending confidential information could be risky. Additionally, the computer user also realizes all e-mails must be screened before forwarding to another person or a distribution list. The computer user is liable for any defamatory or harassing e-mail that is forwarded to a third party. Further, the computer user is also liable for both opening up and forwarding non-work related, unknown or suspicious e-mail that contains a virus. If you are uncertain about the origins of an e-mail or attachment, don't forward it, contact human resources or your in-house attorney.

Deleting E-Mail: When you press the delete key, your e-mail is not deleted. The space is marked as free space but your e-mail is copied on another sector of your hard drive or central server. Your old e-mail can easily be retrieved by a computer forensic specialist or other person from your hard drive, server or other backup device. There is sophisticated software that mines all your e-mail and other documents.

Anonymous E-Mail, Chat Room Discussions or Bulletin Boards: The computer is not allowed to send or forward anonymous or pseudonymous e-mail. It is a direct violation of this policy to send or forward anonymous or pseudonymous e-mail through a remailer or other software or decoding device. Additionally, no chat room or bulletin board will be accessed for sending, forwarding, uploading or downloading unless given written approval by your supervisor or human resources. No chat room or bulletin board will ever be used as a forum for negative, offensive, harassing, defamatory or non-business discussions.

Copyright Infringement: No computer user can upload, download, transmit to another computer, print a hard copy or any way infringe upon the exclusive rights of reproduction, distribution, adaptation, public performance and public display of an on-line or off-line copyrighted work. Not all works on the Internet or Intranet are in the public domain. The computer user must check with the in-house attorney or human resources if there is any uncertainty whether an article or software is copyrighted. Additionally, it is a violation of the Digital Millennium Act to remove any copyright management information (e.g. title, author name, date of registration) There are serious civil and criminal penalties for violating the Federal copyright laws and international copyright treaties.

Trademark Infringement: No symbol, logo, phrase or other trademark can be uploaded, downloaded, transmitted to another computer, used in a web site or hyperlinked to another web site without the express permission of the trademark owner. Trademark infringement carries stiff civil and criminal penalties.

Web Linking, Framing and Metatags: Linking with other web sites is strictly prohibited unless proper authorization is given from human resources or your in-house attorney. When you link with another web site, it can give the appearance you sponsor that site's content. Additionally, no other web site can be framed within your web site unless express permission has been given by human resources or your attorney. Finally, when constructing a web site, the design of Metatags (codes used to identify material to a search engine for indexing) must be authorized by human resources or your in-house attorney.

Passwords: Passwords are for internal use and are not allowed to be distributed to anyone without the express permission of your supervisor or other superior. Passwords are also not to be shared. They are for the exclusive use of the person to whom they have been assigned. Additionally, passwords do not create an expectation of privacy when it comes to employer monitoring.

Off-Site Use Of SBLC Computers: Off-site use of SBLC computers includes but is not limited to home, car, hotel and other off-site locations. You have no expectation of privacy at off-site locations. Additionally, you must adhere to all the same policy restrictions as if you were using the computer on-site. The temptation of informality in your computer usage carries a higher duty of care and responsibility. When using a SBLC computer all off-site computer communication must have a business purpose and all federal and state civil and criminal laws must be respected.

Litigation: In the event of litigation, all computer users are on notice that federal and state civil rules of procedure may allow discovery of all computer hardware and software. This includes but isn't limited to your office computer, laptop, home computer, printers, cell phones and other equipment. Any attempt to damage or destroy evidence in your computer will trigger stiff civil and criminal penalties. If your computer equipment is subpoenaed or you anticipate litigation, contact your in-house attorney or human resources for guidance on how to proceed.

Amendments: This policy may be amended or revised from time to time as need arises. Users will be provided with copies of all amendments and revisions. Any interpretation of this policy as it relates to the computer system will be provided by the Department of Human Resources with guidance from the Information Systems Office and the Attorney's Office.

Waiver: Upon signing this policy, the computer user acknowledges he or she clearly understands the policy and has no further questions as to the content and delivery of this computer use policy. The computer user also affirms that since he or she has no confusion over the content of this policy, there will be no violation of this policy or any other civil or criminal laws relating to computer use. The computer user will indemnify the SBLC and hold harmless for violating SBLC computer policy, which causes; 1) humiliation internally and with the public; 2) disruption of services; and 3) civil or criminal liability. The computer user waives any right to litigate an inadequate training claim or other negligence claim against SBLC for not clearly understanding this computer use policy.

Name (Printed) _____ Date _____

Work Site _____ Job Title _____

Signature _____

District Office Use Only	
Account Name :	_____ Date: _____
Signature:	_____
<input type="checkbox"/>	Skyward Student Account

Form Date: 09/13/2007