

PLEASE READ THIS DOCUMENT CAREFULLY BEFORE SIGNING. NO VOLUNTEER WILL BE GIVEN INTERNET ACCESS UNLESS HE OR SHE SIGNS THIS POLICY. THE POLICY IS DESIGNED TO CLEARLY ANNOUNCE THE POSSIBLE RISKS OF USING THE INTERNET. THE SCHOOL DISTRICT PROVIDES INTERNET FILTERS AND TAKES EVERY REASONABLE PRECAUTION TO ENSURE THE INTERNET IS SAFE. HOWEVER, VOLUNTEERS MAY ATTEMPT TO BYPASS THE SCHOOL FILTERS OR USE THEIR HOME COMPUTER TO EXPOSE OTHERS TO THE FOLLOWING RISKS:

- Sharing offensive websites with other persons
- Sending and receiving inappropriate e-mail, blogs and other prohibited messages
- Sharing offensive material created at home or in other remote locations
- Sending or receiving libelous electronic messages
- Sending or receiving HIPAA- or FERPA-protected health or educational information
- Illegally using another person's password or e-mail address
- Engaging in the violation of criminal and civil laws
- Illegally uploading or downloading copyrighted material
- Using someone's picture in a false light
- Violating a person's financial or academic privacy

The Santa Rosa County School Board of Education provides internet access to volunteers for educational purposes only. DUE TO CURRENT FEDERAL LAWS YOU HAVE LITTLE OR NO EXPECTATION OF PRIVACY WHEN USING THE INTERNET AT SCHOOL (OR AT HOME WHEN RELATED TO SCHOOL BUSINESS, e.g., writing about students, employees, or other volunteers). The district is authorized to do random audits of volunteer browser histories. Volunteers should understand that all Internet usage is monitored and recorded.

Misuse of the Internet violates school board policy and subjects you to school disciplinary procedures. Additionally, you may incur civil and criminal penalties under Florida and Federal law for misuse of the Internet. Some of the misuses are as follows but not limited to:

- Using proxy sites to avoid the district filter
- Using district-provided computer equipment for personal use
- Using district provided computer equipment for personal or business profit
- Using district provided computer equipment for criminal purposes
- Using district provided computer equipment for civil rights violations
- Using district provided computer equipment to send defamatory material
- Using district provided computer equipment for violation of a person's privacy
- Using district provided computer equipment to share ID's and passwords
- Using district provided computer equipment to share passwords with students
- Using district provided computer equipment to share static IP addresses with students
- Using district provided computer equipment to commit sexual harassment
- Using district provided computer equipment to threaten death or bodily harm
- Using your own portable devices to distribute offensive material on school grounds
- Using district provided computer equipment to violate copyright laws

General Network- and Internet-Related Acceptable Use

- 1) All troubleshooting must go through the site Technology Contact. Volunteers must not ask students to troubleshoot computers.
- 2) Users must ensure the security of any account issued in their name. Giving students access to a volunteer account is a violation of School Board policy, HIPAA and FERPA. Confidential information such as Social

Security number, password, or medical information, is private and requires protection with the highest levels of security, as prescribed by applicable laws, regulations, and standards. Measures taken to ensure the protection of confidential or sensitive information include but are not limited to a) using strong passwords (i.e., at least eight letters and numbers and including a combination of at least three of the following: uppercase letters, lowercase letters, number, and symbols (e.g., !, @, ^); b) securing your workstation each time you leave it by locking it or logging off, and c) reporting suspected incidents of security violations.

~~(dtp/adden01a.pdf page 3 Data Security section)~~

- 3) Social media activities that are not work-related (e.g., Facebook games) should not interfere with work commitments and should not be conducted during work hours. Refer to School Board Policy 6.38.
- 4) District volunteers shall use caution and good judgment when using electronic communications and social networking sites. Any information posted to or communicated through a social networking site shall not bring disfavor, embarrassment or condemnation to employees, students, or the school district. ~~For the complete Social Networking Policy, see Telecommunications Policies & Procedures.~~
- 5) School or district-related web sites (including blogs, wikis, nings, etc.) must be maintained on a district-owned Web server or district-approved alternate host (www.santarosa.k12.fl.us/pdc/docs/dtp/adden07c.pdf). Teachers must pre-approve all content uploaded by students. All district policies and guidelines shall be met. ~~(Addendum 1A-Telecommunication Policies & Procedures)~~
- 6) Obtain permission from the district Web Administrator to redirect school web pages to sites outside of Santa Rosa School District's control with the exception of district-approved alternate sites.
- 7) Create hyperlinks only to sites approved by the official school/site Web Manager(s).
- 8) Email, web pages, and other Internet communications guidelines should be adhered to as follows:
 - a) Volunteers will not be given a district email account.
 - b) Use of district-provided equipment to access email and websites for non-educational purposes is prohibited. Examples include but are not limited to: jokes, chain letters, political advertisements, sales or profit-making activities, religious passages or any word or phrase that has religious connotations, and inspirational stories.

Relevant School Board Policy

- School Board Policy (<http://www.santarosa.k12.fl.us/policy/>)
- ~~Telecommunications Plan Policies and Procedures (<http://www.santarosa.k12.fl.us/pdc/docs/>)~~

Upon signing this document you affirm that it is not reasonable that the Santa Rosa school district can directly supervise you every minute you are on the computer. Therefore, you agree that when you are not directly supervised, you will obey all school computer use policies, civil and criminal laws. In the event you are receiving computer messages threatening death, bodily harm, or destruction to property, you agree to report this event immediately to both law enforcement and the Santa Rosa School County School District.

I, (please print name) _____, have read and agree to abide by Santa Rosa County School Board's Acceptable Use Policies for Volunteers. I understand that should I violate these policies, my right to use these resources may be revoked, and my volunteer status may be revoked.

Volunteer Signature

Date

Volunteer School/Site

Give signed original to Site Administrator or Designee
Keep signed copy for your records.