

Related Entries: (Not identified at this time)

### Acceptable Use Policy Governing Internet and Technology Access

The principal of a school or the supervisor of a department shall be responsible for ensuring that the following procedures are followed for governing Internet and technology access. Failure to adhere to these regulations shall result in suspension and/or revocation of access to District information resources pending formal investigation and could result in termination of employment (staff) or suspension/expulsion (student) from the School District.

- (1) The School District of Lee County provides technology resources to its students and staff for educational and administrative purposes. The use of these technology resources is a privilege, not a right and, as such, is subject to revocation and appropriate discipline by the School District administration at any time for abusive conduct or violation of any of the requirements of this policy.
- (2) All users are prohibited from:
  - (a) Deliberate access or transmission of obscene, indecent, abusive, defamatory or otherwise offensive material in any form including improper use of telecommunication services or technology, and posting inappropriate information on the web, during or after school/work hours that may interfere with the school/work environment.
  - (b) Transmission of material endorsing or opposing any candidate for political office. Communications by the Board's legislative liaison to provide information and encourage action on pending legislation affecting the School District and the forwarding of such communications are not included in this prohibition, if approved by the Superintendent or designee.
  - (c) Transmission of religious material.
  - (d) Deliberate or malicious attempts to harm, destroy, or steal data on any system on the network and/or Internet.
  - (e) Unauthorized installation, storage or distribution of copyrighted software or materials on any School District electronic information system. All users of telecommunication and network resources shall adhere to current copyright law.

- 45 (f) Reposting personal communications without the author's prior consent.  
46  
47 (g) Using the network for personal financial gain, or any commercial or illegal  
48 activity. The Superintendent or designee may approve commercial  
49 advertising on the District website and through e-mail distribution to all staff  
50 when such advertising is not obscene, indecent, abusive, or defamatory and  
51 does not advertise a product or service appropriate only for adult use.  
52 Additionally, the advertiser must provide a benefit to the school or District or  
53 school or District employee. The school principal may approve advertising on  
54 the school website and through e-mail distribution to all school staff on the  
55 same terms. No pop-up advertising will be allowed on the school or District  
56 website.  
57  
58 (h) Deliberate spread of computer "viruses."  
59  
60 (i) Attaching/installing/adding personally owned software, computer and/or other  
61 electronic devices to any District network without written permission from  
62 District administration.  
63  
64 (3) As a condition of use of District information resources, all users understand and  
65 agree with the following:  
66  
67 (a) The District complies with the Children's Internet Protection Act (CIPA) and in  
68 doing so ensures that during the school day and school activities:  
69  
70 1. Access by users to inappropriate matter on the Internet and World  
71 Wide Web is not permitted under any circumstances. For all users,  
72 "inappropriate matter" includes child pornography and visual  
73 depictions of obscenity. For users under 17 years of age,  
74 "inappropriate" also includes matters harmful to minors as defined by  
75 CIPA.  
76  
77 2. The safety and security of minors when using electronic mail, chat  
78 rooms, and other forms of direct electronic communication is  
79 protected.  
80  
81 3. Unauthorized access, including "hacking" and other unlawful activities  
82 by minors is prohibited.  
83  
84 4. Unauthorized disclosure, use and dissemination of any personal  
85 information regarding minors are prohibited.  
86  
87 5. Technology protection measures are in place, which are designed to  
88 restrict user access to inappropriate matters.  
89

- 90 6. All students receive instruction regarding appropriate on-line behavior,  
91 including interacting with other individuals on social networking sites  
92 and in chat rooms and cyber bullying awareness and response.  
93
- 94 (b) The District has the right to review any materials stored in District computers  
95 and electronic systems. Any right of privacy that users of District information  
96 resources may have in and to such material is waived. All information  
97 transmitted through the telecommunication and network resources of the  
98 District are considered District property.  
99
- 100 (c) The District can edit or remove any materials, which it believes may be  
101 unlawful, obscene, indecent, abusive or in any way objectionable.  
102
- 103 (d) The use of the Internet is for educational purposes only. Students are not  
104 allowed to access the Internet without supervision. The District provides such  
105 supervision only during the school day and school activities. Parents/  
106 guardians are responsible for such supervision outside the school day and  
107 school activities.  
108
- 109 (e) All information and services contained on the District computers are placed  
110 there solely for general educational purposes.  
111
- 112 (f) System passwords are the responsibility of each individual user. Passwords  
113 shall not be shared with others and shall be kept secure at all times. Failure  
114 to secure passwords shall result in the revocation of network access.  
115
- 116 (4) Any attempt to damage or impair the information resource network of the District,  
117 such as e-mail bombardment, transmission of chain letters, virus hoaxes, "spoofing"  
118 of header or identifiable information regarding the sender, hacking or "sniffing," shall  
119 result in revocation of network access and may subject the user to disciplinary  
120 and/or legal action.  
121
- 122 (a) Users of telecommunication and network resources shall conduct themselves  
123 in an ethical and legal manner.  
124
- 125 (b) Only the person authorized to have access by the School District shall have  
126 access to District resources such as e-mail, mainframe and other electronic  
127 information resources.  
128  
129

130 **STATUTORY AUTHORITY:** 1001.42, 1001.43, F.S. and 20 USC Section 9134  
131

132 Adopted: 1/6/09

133 Revised: 3/6/12