



POLICY 2.50

5-D I recommend that the Board approve development of the proposed **new** Policy 2.50, entitled "Third Party Use of Technology."

[Contact: Deepak Agarwal, PX 48773 and Larry Padgett, PX 48830.]

Development

CONSENT ITEM

- This Policy sets forth terms and conditions as well as standards and guidelines for the acceptable uses of Palm Beach County School District technology resources and other technology by third parties (as defined in the policy including volunteers, contractors, and vendors) when authorized to use District technology and when conducting District business.
- It also addresses: third party use of e-signatures and electronic notarizations when authorized; compliance required by third parties; and implementation procedures and policy enforcement which includes the right of terminating access and other actions including civil liability.

See Item 5A/Policy 8.123 for the referenced IT User Standards and Guidelines Manual.

POLICY 2.50

THIRD PARTY USE OF TECHNOLOGY

- 1
2
3 1. **Purpose.** -- The purpose of this Policy is to set forth terms and conditions as well
4 as standards and guidelines for the acceptable uses of Palm Beach County School
5 District technology resources and other technology by third parties when
6 conducting District business and authorized to use District technology. The Policy
7 also provides for third party use of e-signatures and electronic notarizations when
8 authorized. This Policy does not prohibit or restrict public access to inspect data
9 and information on publicly available District technology resources.
- 10 2. **Definition**— A third party is a: Volunteer, contractor, vendor, governmental entity,
11 individual or private organization transacting business with or providing products,
12 services or support to the District or other person or entity who is considered part of
13 the School District. Additional definitions appear within the District's Information
14 Technology (IT) User Standards and Guidelines Manual, as described below.
- 15 3. **General Standards of Appropriateness.** -- When using District technology
16 resources, applications, databases, and supplies, all third parties shall adhere to
17 the standards established by this Policy, all applicable laws, regulations, rules, and
18 the District's Information Technology (IT) User Standards and Guidelines Manual
19 ("Manual"). This Manual is specifically incorporated by reference into this policy
20 and is located on the District's IT Security web site at:
21 <http://www.palmbeachschools.org/it/security.asp>.
- 22 4. Except as permitted above in paragraph 1, third parties shall use District
23 technology resources, including, but not limited to computers, networks, copiers,
24 biometric record readers, and communication devices such as cell and office
25 phones, personal digital assistants (PDAs) and facsimile machines, only for
26 District-related activities and when authorized and allowed by an appropriate
27 District representative.
- 28 5. Third parties using the Internet in any form through the District's non-public network
29 must submit to Superintendent's designee (or, if the form is available and can be
30 transmitted electronically, to the District) a completed and signed Third Party
31 Internet/Intranet Services Acknowledgement and Consent form (PBSD 2359). The
32 third-party shall sign and submit this form before initial use of the Internet through
33 the District's non-public network.
 - 34 a. The consent form shall state and the third party shall acknowledge that there
35 is only a limited expectation of privacy to the extent required by law for the
36 third party related to his/her use of District technology resources. The District
37 may monitor a third party's use of District technology for good cause, such as

- 38 ensuring that their use is authorized; for management of the system; to
39 respond to a records request; to facilitate protection against unauthorized
40 access; verifying security procedures, survivability and operational security;
41 investigating misconduct, compliance with School Board policies, a possible
42 security incident, or computer performance.
- 43 b. The consent form shall further state: Before using the District's technology
44 resources, where applicable, users shall become familiar with the Fla. Admin.
45 Code Sections 6B-1.001 and 6B-1.006, including the provisions prohibiting
46 harassment and discrimination, defamation, use of institutional privileges for
47 personal gain, and improper disclosure of confidential information; Fla. Stat. §
48 112.313, including the duty to avoid improper use or disclosure of "information
49 not available to members of the general public and gained by reason of [their]
50 official position for [their] personal gain or benefit or for the personal gain or
51 benefit of any other person or business entity", and School Board Policy
52 8.121 on the use of copyrighted materials. All third party users shall abide by
53 these provisions when using the District's technology resources.
- 54 c. Third Parties are advised that many District technology resources, including
55 but not limited to laptops and desktops, may contain input systems such as
56 web cameras and microphones which can be remotely controlled to turn them
57 on and off. The District will not utilize any such input systems remotely unless
58 consistent with the law.
- 59 6. The District authorizes third parties to use District technology resources,
60 applications, and databases for the parties' assigned responsibilities when allowed
61 by an appropriate District representative. Third parties shall use these resources to
62 enhance their performance of District activities. Principals and department heads
63 are to follow District standards to ensure accountability of third party's use of these
64 resources to support academic and business functions.
- 65 7. Third party user account/passwords with the District or with another entity
66 approved by the District can be used as set forth in the Manual to:
- 67 a. Electronically sign District documents by e-signature.
- 68 b. Provide access to the third party's personal information.
- 69 c. Make binding legal obligations.
- 70 d. Access District files or records.
- 71 8. All passwords are to be treated as sensitive and confidential information and shall
72 not be shared with anyone but the third party to whom they were assigned. All
73 users are responsible for all activity that occurs for user accounts that have been
74 assigned to them.

- 75 9. Compliance.— When using District technology resources, applications,
76 databases, and supplies, in addition to adhering to the standards set forth in the
77 Manual and above in this Policy, all users must observe that:
- 78 a. Any information generated through a computer, stored on hard disks,
79 electronically mailed, or handled as e-mail, if it meets the definition of a public
80 record, is subject to the District’s retention schedule and Florida law
81 concerning public records, as explained in Policy 2.041. The District’s
82 Retention Schedule can be found at:
83 <http://www.palmbeach.k12.fl.us/Records/Text/RetnSchd.doc>. Third parties, are
84 allowed to communicate by e-mails through services provided by the District
85 but are prohibited from engaging in text messaging, instant messaging,
86 tweeting and other methods of instant electronic communication if the
87 messages must be retained as public records in accordance with the District’s
88 Retention Schedule.
- 89 b. Certain District data (including all student and employee data) may be subject
90 to special privacy restrictions and therefore cannot be treated as “public
91 records.” All third party users shall agree to maintain the security and privacy
92 of that data/information as specified by District policy and applicable State and
93 Federal laws with the understanding that District non-public data is the
94 exclusive property of the District and shall be maintained as such. This data
95 shall not be copied or modified.
- 96 c. Third parties will accept all risks and responsibilities associated with using
97 and/or connecting approved non-District resources or equipment to District
98 technology resources. In regard to such non-District resources or equipment,
99 third party shall agree to the following:
- 100 i. In the event of a security breach, authorize the District to take immediate
101 action to reduce the District’s exposure which may include a scan of third
102 party equipment.
- 103 ii. Further authorize the District to perform inspection of third party
104 resources as deemed necessary to ensure the safety and security of
105 District data and/or technology resources, and to ensure that any
106 software or other similar intellectual property is duly licensed for use.
- 107 iii. Understand the District will require virus-detection software in accordance
108 with its own specifications, and agree to comply with virus protection and
109 scanning requirements.
- 110 iv. Indemnify and hold the District harmless from damage incurred as a
111 result of connecting approved non-District resources or equipment.
- 112 d. The willful and knowing unauthorized use, modification, alteration,

113 dissemination, or destruction of District information technology resources or
114 databases is considered a violation of this Policy and the District may impose
115 sanctions, up to and including termination of relationship between the School
116 District and third party or denial or restriction of access to District technology
117 resources. The District procedures may request reimbursement to the District
118 for the actual cost of damages from the third party. If the third party does not
119 make payment, the School Board may institute a civil action for damages to
120 hold the third party liable. Moreover, this conduct may constitute a computer-
121 related crime punishable under Fla. Stat. ch. 815.

122 e. All third parties who have access to or may have access to personally
123 identifiable student information shall adhere to all standards included in the
124 Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; the
125 IDEA and its regulations at 20 U.S.C. § 1417(c) and 34 C.F.R. § 300.572; Fla.
126 Stat. §§1002.22 and 1002.221, School Board Policy 5.50, and other applicable
127 laws and regulations, as they relate to the release of student information. Third
128 parties shall not use access to student records information for personal gain
129 and shall use and release student information only as authorized by law. Third
130 parties cannot, by any means, take, obtain, receive, acquire, or capture any
131 District data, meta data, or information from any District system for any
132 purpose without written consent from the District.

133 f. Intranet and Internet Resources, phones, text messaging, instant messaging,
134 and e-mail, when utilized, shall be used in performance of District business
135 and shall not be used to send abusive, threatening, or harassing messages.
136 Third parties shall not send communications where the meaning of the
137 message, or its transmission or distribution, would be illegal under state or
138 federal statutes, federal regulations, or state rules; or unethical under or
139 violative of Fla. Stat. ch. 112, Chapter 6B-1 of the State Board of Education
140 rules, or School Board Policies, including Policies 5.001, 5.002, 5.81 and 3.02
141 (to the extent these are applicable).

142 g. All software on computers must be licensed. Third parties are responsible for
143 using software in compliance with restrictions that apply to those licensing
144 agreements.

145 h. Users shall not make or facilitate the distribution of unauthorized copies of
146 software. Modifications cannot be made to any software without the
147 authorization of the copyright holder. The copyright legend or notice shall not
148 be removed from the software or any of its documentation.

149 10. Forms: The PBSB forms mentioned in this Policy or within the Manual are
150 incorporated herein by reference, as part of this policy and can be found on the
151 District's Records Management Web site for forms, located at
152 <http://www.palmbeach.k12.fl.us/Records/FormSearch.asp>.

153 11. **Implementation.** -- The Superintendent or designee is authorized to issue bulletins
154 and administer procedures regarding the use of information technology in the
155 District in accordance with the standards set forth in this Policy including the
156 Manual.

157 12. **Enforcement.** -- Any third party failing to comply with this Policy or its
158 implementing procedures and standards may be subject to consequences up to
159 and including termination of access to District technology resources, requiring
160 reimbursement to the District, and civil or criminal liability. IT has the authority to
161 take reasonably necessary immediate actions to protect District technology
162 resources.

163 STATUTORY AUTHORITY: Fla. Stat. §§ 1001.32(2); 1001.41(2); 1001.42(26);
164 1001.43(1)

165 LAWS IMPLEMENTED: Fla. Stat. §§ 1001.32(2); 1001.43(3); 1001.42(8) & (9);
166 1003.31; 1006.28(1)

167 HISTORY: ___/___2010

Legal Signoff:

The Legal Department has reviewed proposed Policy 2.50 and finds it legally sufficient for development by the Board.

Attorney

Date



THE SCHOOL DISTRICT OF PALM BEACH COUNTY

Third-Party Internet/Intranet Services Acknowledgement and Consent

This form is to be used by the third-parties to request access to Internet and intranet services through the networking facilities in the District. This form must be completed and signed by each third-party that wishes to use any Internet or intranet services, including district e-mail, world-wide web and other Internet services. Third-parties must agree to the conditions below to gain access to Internet or District intranet services. Third-parties must read and be familiar with the IT User Standards and Guidelines Manual available at <http://itsecurity.palmbeach.k12.fl.us>.

Acceptable Use and Non-Disclosure Statement

1. I have read, understand, and am responsible for actions described in *Board Policy 2.50, Third-Party Use of District Technology* at http://www.palmbeach.k12.fl.us/policies/2_50.htm and the IT User Standards and Guidelines Manual at <http://itsecurity.palmbeach.k12.fl.us>.
2. I acknowledge that a very limited expectation of privacy exists to the extent required by law for me as a third-party related to my use of District technology resources. District technology resources may be monitored for all lawful and good cause purposes. Use of these resources constitutes consent for the District to monitor these resources for these purposes. I further acknowledge that the District may retrieve and/or disclose, as allowed by law, all messages stored by the District or an outside entity on its behalf.
3. I acknowledge that before using the District's technology resources, I will be familiar with the District's employee code of conduct (School Board Policy 3.02) as well as Fla. Admin. Code Sections 6B-1.001 and 6B-1.006, including the provisions prohibiting harassment and discrimination, defamation, use of institutional privileges for personal gain, and improper disclosure of confidential information; Fla. Stat. § 112.313, including the duty to avoid improper use or disclosure of "information not available to members of the general public and gained by reason of [their] official position for [their] personal gain or benefit or for the personal gain or benefit of any other person or business entity", and School Board Policy 8.121 on the use of copyrighted materials.
4. District technology resources, applications, and databases will be used only for my assigned duties and responsibilities in performance of District business as stated in Policy 2.50 and its Manual.
5. All activities performed while using my District computer account will be attributed to me and no one else.
6. My District computer account may be used by me to electronically sign District documents and make binding legal obligations for transactions, if I am authorized to do so. My account may also be used to access and update my personal information in District information systems.
7. I acknowledge my intent to be bound by documents I sign electronically by the method described above in paragraph 6.
8. All passwords assigned to me will be kept confidential and I will not disclose them to anyone.
9. Non-compliance with the above conditions may result in consequences, including loss of privileges, or termination of agreement.

By signing below, I hereby acknowledge that I have read and understand the terms and conditions of this Acknowledgment and Consent, the statements are true and correct, and I agree to be bound by the terms and conditions.

Print Name of Third Party

Signature of Third Party

Date