

CHAPTER 3.00 – SCHOOL ADMINISTRATION

3.022

THIRD PARTY USE OF TECHNOLOGY

POLICY:

The purpose of this Policy is to set forth terms and conditions as well as standards and guidelines for the acceptable uses of Dixie County School District technology resources and other technology by third parties when conducting District business and authorized to use District technology. The Policy also provides for Third Party use of e-signatures and electronic notarizations when authorized. This Policy does not prohibit or restrict public access to inspect data and information on publicly available District technology resources.

- (1) Procedures on Definitions – These definitions apply to terms within this Policy.
 - (a) A third party is a: volunteer, contractor, vendor, governmental entity, individual or private organization transacting business with or providing products, services, or support to the district or other person or entity who is considered part of the School District.
 - (b) Defamation – Defamations, including libel, has been interpreted to mean that a plaintiff must show that (1) the defendant published an unprivileged false statement about the plaintiff, (2) to a Third Party, and (3) the falsity of the statement caused injury to the plaintiff.
 - (c) Harmful to Minors – Any reproduction, imitation, characterization, description, exhibition, presentation, or representation, of whatever kind of form, depicting nudity, sexual conduct, or sexual excitement when it: (a) Predominantly appeals to a prurient, shameful, or morbid interest; (b) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material or conduct for minors; and (c) taken as a whole is without serious literary, artistic, political, or scientific value for minors.
 - (d) Obscene – The status of material which: (a) The average person, applying contemporary community standards, would find, taken as a whole, appeals to the prurient interest; (b) Depicts or describes, in a patently offensive way, sexual conduct as specifically defined herein; and (c) Taken as a whole lacks serious literary, artistic, political, or scientific value.

- (2) General Standards of Appropriateness - When using District technology resources, applications, databases, and supplies, all third parties shall adhere to the standard established by this policy, all applicable laws, regulations, rules. When using District technology, including but not limited to applications, databases, websites, and supplies, third parties shall adhere to the standards established by this Policy. All applicable laws, regulations, rules, applicable School Board policies, including Policy 5.19 Student Records Policy. May be found at:
<http://dixieschools.dixie.k12.fl.us/SM%20Documents/Board%20Policies/policy%205.19.pdf>

CHAPTER 3.00 – SCHOOL ADMINISTRATION

- (3) Except as permitted above in paragraph 1, third parties shall use District technology resources, including, but not limited to computers, networks, copiers, biometric record readers, and communication devices such as cell and office phones, smart phones, mobile devices and facsimile machines, only for District-related activities and when authorized and allowed by an appropriate District representative.
- (4) Third parties using the Internet in any form through the District's non-public network must submit to Superintendent's designee (or, if the form is available in can be transmitted electronically to the District) a completed and signed Third Party Internet Service Acknowledgement and Consent form. The Third Party shall sign and submit this form before initial use of the Internet through the District's non-public network.
 - (a) The consent form shall state and the Third Party shall acknowledge that there is only a limited expectation of privacy to the extent required by law for Third Party related to his/her use of District technology resource. The District may monitor at Third Party's use of District technology for good cause by GPS and other technologies that reside on District equipment and assets, such ensuring that their use is authorized: for management of the system; to respond to a records request; to facilitate protection against unauthorized access; verifying security procedures, survivability and operational security; investigating misconduct; compliance with School Board policies; a possible security incident, or computer performance.
 - (b) The consent form shall further state: Before using the District's technology resources, where applicable, users shall become familiar with the Florida Administrative Code Sections 6A-10.080 and 6A-10.081, including the provisions prohibiting harassment and discrimination, defamation, and libel, prohibiting matters that are obscene, hateful, or harmful to minors, - use of institutional privileges for personal gain, in the improper disclosure of confidential information; Florida Statute 112, .313, including the duty to avoid improper use of 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 3.08 on the use of copyrighted materials. All Third Parties users shall abide by these provisions when using the District technology resources.
 - (c) Third Parties are advised that many District technology resources, including but not limited to laptops and desktops may contain input systems, such as web cameras and microphone which can be remotely controlled to turn them on and off. The District will not utilized any such input systems remotely unless consistent with the law.

CHAPTER 3.00 – SCHOOL ADMINISTRATION

- (5) The District authorizes Third Party's to use District technology resources, applications, and databases for the parties' assigned responsibilities when allowed by appropriate District representative. Third Parties shall use these resources to enhance their performance of District activities. Principals and department heads are to follow District standards to ensure accountability of Third Party's use of these resources to support academic and business functions.
- (6) Third Party user account/passwords with the District or with another entity approved by the District can be used as set forth in the District policy 8.341 to:
 - (a) Electronically sign District documents by e-signature.
 - (b) Provide access to the Third Party's personal information.
 - (c) Make binding legal obligations.
 - (d) Access District files or records.All passwords are to be treated as sensitive and confidential information and shall not be shared with anyone but the Third Part to whom they were assigned. All users are responsible for all activity that occurs for user accounts that have been assigned to them.
- (7) The District uses various measures to protect its network and information resources and its users; however, the District cannot guarantee that security incidents and hacking will not happen. The District accepts no responsibilities for harm caused directly or indirectly by the user of its network and information resources.
- (8) Compliance – When using District technology resources, applications, and databases, in addition to adhering to the standards set forth in the Policy 8.341 and above in this Policy:
 - (a) All users must retain communication or information generated through a computer or electronic device that meets the definition of public record. Retention is required subject to the District's Records Retention Schedule, records holds and Florida law concerning public records, as explained in School Board Policy 8.26. The District's Retention Schedule can be found at: <http://dixieschools.dixie.k12.fl.us/admin/BoardPolicy081407/policy8.26.pdf>. These communications include but are not limited to email, text messages, instant messages, tweets, and similar instantaneous methods of communication. Third Parties are allowed to communicate by emails through services provided by the District but shall not communicate in text messaging, instant messaging, tweeting or other methods of instant electronic communications if the messages cannot be retained as required by the District Retention Schedule. Third Parties are not allowed to communicate

CHAPTER 3.00 – SCHOOL ADMINISTRATION

- through transitory messages, as defined in the District's Records Retention Schedule.
- (b) Certain District data (including all student and employee data) may be subject to special privacy restrictions and therefore cannot be treated as "public records." All Third Party users shall agree to maintain the security and privacy of that data/information as specified by District policy and applicable State and Federal laws with the understanding that District non-public data is the exclusive property of the District and shall be maintained as such. This data shall not be copied or modified.
 - (c) Third Parties will accept all risk and responsibilities associated with using and/or connecting approved non-District resources or equipment to District technology resources. In regards to such non-District resources or equipment, Third Party shall agree to the following:
 - 1) In the event of a security breach, authorize the District to take immediate actions to reduce the District's exposure which may include a scan of Third Party equipment.
 - 2) Further authorize the District to perform inspection of Third Party resources as deemed necessary to ensure the safety and security of District data and/or technology resources, and to ensure that any software or other similar intellectual property is duly licensed for use.
 - 3) Understand the District will require virus-detection software in accordance with its own specifications, and agree to comply with virus protection and scanning requirements.
 - 4) Indemnify and hold the District harmless from damage incurred as a result of connecting approved non-District resources or equipment.
 - (d) The willful and knowing unauthorized use, modification, alteration, dissemination, or destruction of District information technology resources or databases is considered a violation of this Policy and the District may impose sanctions, up to and including termination of relationship between the School District and Third Party or denial or restriction of access to District technology resources. The District procedures may request reimbursement to the District for the actual cost of damages from the Third Party. If the Third Party does not make payment, the School Board may institute a civil action for damages to hold the Third Party liable. Moreover, this conduct may constitute a computer-related crime punishable under Florida Statute Chapter 815.
 - (e) All Third Parties who have access to or may have access to personally identifiable student information shall adhere to all standards included in the Family Educational Rights Privacy Act (FERPA), 20 U.S.C. 1232g; the Individual with Disabilities Education Act (IDEA) and its regulation at 20 U.S.C 1417 and 34 C.F.R. 300.623; Florida Statute 1002.22 and 1002.221; School Board Policy 5.19, and other applicable laws and regulation, as they relate to the release of student information. Third parties shall not use access to student records information for personal gain and shall use and release

CHAPTER 3.00 – SCHOOL ADMINISTRATION

- student information only as authorized by law. Third Parties cannot, by any means, take, obtain, receive, acquire, or capture any District data metadata, or information from any District System for any purpose without written consent from the District.
- (f) Intranet and Internet Resources, phones, text messages, instant messaging, and e-mail, when utilized, shall be used in performance of District business and shall not be used to send abusive, threatening, discriminatory, libelous, obscene, hateful, harmful to minors, or harassing messages. Third Parties shall not send communications where the meaning of the message, or its transmission or distribution, would be illegal under state or federal statutes, federal regulations, or state rules; or the message or transmission is unethical under or in violation of Florida Statute Chapter 112, State Board of Education rules 6A-10.080 and 6A-10.081.
 - (g) All software on computers must be licensed. Third Parties are responsible for using software in compliance with restrictions that apply to those licensing agreements.
 - (h) Users shall not make or facilitate the distribution of unauthorized copies of software. Modification cannot be made to any software without the authorization of the copyright holder. The copyright legend or notice shall not be removed from the software or any of its documentation
 - (i) Use of non-District approved cloud services is prohibited. District approved storage services may be identified as contracted services. If the Third Part is allowed to access student data, the Third Part shall not allow the use of student data or any purpose other than as stated in the contract with the District.
 - (j) If a Third Party is issued a District email account then the Third Party shall identify themselves as a Third Party and not a District employee in email signatures line with the following statement, "Third Party to the School District of Dixie County – non-School District employee".
- (9) Implementation – The Superintendent or designee is authorized to issue bulletins and administer procedures regarding the use of information technology in the District in accordance with the standards set forth in this Policy.
- (10) Enforcement – Any Third Party falling to comply with this Policy or its implementing procedures and standards may be subject to consequences up to and including termination of access to District technology resources, requiring reimbursement to the District, and civil or criminal liability. IT has the authority to take reasonably necessary immediate actions to protect District technology resources.

CHAPTER 3.00 – SCHOOL ADMINISTRATION

STATUTORY AUTHORITY: 1001.32 (2); 1001.41 (2); 1001.42 (27); 1001.43 (1), F.S.

LAWS IMPLEMENTED: 1001.32 (2); 1001.43 (3); 1001.42 (8) and (9); 1003.31; 1006.28 (1), F.S.

History:

Adopted: November 22, 2016 Revision Date(s): Formerly:
--