

Yancey County School Board Policy

BOARD OPERATIONS

USE OF PERSONAL TECHNOLOGY TO CONDUCT SCHOOL BUSINESS

Policy Code: 3228 / 7323

December 16, 2019

The board recognizes that employees may use a variety of personal technology devices and accounts in their personal lives. At times, it may be convenient for employees to use their personal technology devices and accounts to conduct school business. Although such use of personal technology devices and accounts may be convenient, it is likely to produce a conflict between employees' interests and the school's obligations: employees ordinarily expect privacy in their personal technology devices and accounts, but the school is legally obligated to preserve certain school business-related electronically stored information ("ESI").

School business-related ESI (including text messages and e-mails) sent and/or received by an employee using a personal technology device or account may constitute public records or student education records, and as a result may require retention and disclosure by the school system. In the event of litigation, school business-related ESI located on a personal technology device or account may be subject to discovery and a litigation hold.

A. Limitations on Use

Unless otherwise authorized by a BYOT (Bring Your Own Technology) initiative, employees are expected to use school-controlled technology devices and accounts for conducting school business and storing school business-related ESI when such devices and accounts are readily available. Any use of personal technology devices and accounts is subject to this policy and all other relevant board policies, including but not limited to policy [3225/4312/7320](#), Technology Responsible Use, and policy [7335](#), Employee Use of Social Media.

1. Personal Technology Devices

For purposes of this policy, "personal technology device" means a technology device that is not under the control of the school system and which the school system does not have the ability to access without the employee's assistance. This definition includes, but is not limited to, computers, phones, tablets, and other technological devices that are owned or leased by an employee.

Use of personal technology devices to conduct school business or to store school business-related ESI is authorized only when (1) done in accordance with an official BYOT program; (2) the use is occasional and incidental to the regular use of school-controlled technology devices; or (3) the superintendent or designee has pre-approved in writing the employee's regular use of personal technology for conducting school business and/or storing school business-related ESI.

For purposes of this policy, “personal external storage device” means a device that has a primary purpose of storing data, is not under the control of the school system, and which the school system does not have the ability to access without the

employee’s assistance. Personal external storage devices constitute personal technology devices for purposes of this policy, but are subject to the following additional limitation: employees are prohibited from storing school business-related ESI on personal external storage devices, including, but not limited to, external hard drives, USB flash drives, flash memory cards, DVDs, compact discs, or magnetic tape, unless specifically authorized to do so by the superintendent or designee in writing.

2. Personal Accounts

For purposes of this policy, “personal account” means an account that is not under the control of the school system and which the school system does not have the ability to access without the employee’s assistance. This definition includes, but is not limited to, personal email accounts, social media sites, and online file storage services (e.g., file hosting services, cloud storage services, or online file storage providers that host user files via the Internet).

Employees are prohibited from using personal accounts to conduct school business or to store school business-related ESI unless specifically authorized to do so by the superintendent or designee in writing.

B. School System Access to School Business-Related ESI on Employees’ Personal Technology Devices and Accounts

Any school business-related ESI stored on an employee’s personal technology devices or accounts is property of the school system. Employees shall transfer to an appropriate custodian all school business-related ESI upon request of the superintendent or designee and upon leaving employment. Employees shall cooperate with school officials in accessing any school business-related ESI stored on personal technology devices or accounts.

Employees are cautioned that using personal technology devices or accounts to conduct school business or to store school business-related ESI will significantly reduce their expectation of privacy in those devices or accounts. If an employee uses a personal technology device or account to conduct school business or to store school business-related ESI, an inspection of the employee’s device or account may be necessary to ensure that all public records and education records are preserved.

By using personal technology devices or accounts to conduct school business or to store school business-related ESI, employees are deemed to consent to the school system accessing and inspecting such devices or accounts to gather school business-related ESI

and ensure that all public records and education records are preserved. If school officials have a reasonable basis to conclude that school business-related ESI is stored on an employee's personal technology device or account, a reasonable inspection of the employee's device or account may be performed in order to retain any public records or education records required to be retained by law and/or board policy. Such an inspection shall be made only after consultation with the board attorney.

C. Required Notices and Consent

All employees must be informed annually of the terms of this policy and the methods by which they may obtain a copy of this policy. Employees must sign a statement indicating that they understand and will comply with the requirements of this policy.

Legal References: U.S. Const. amend IV; Stored Communications Act, 18 U.S.C. 2701, *et seq.*; Computer Fraud and Abuse Act, 18 U.S.C. 1030; G.S. 14-454, -458

Cross References: Technology in the Educational Program (policy [3220](#)), Technology Responsible Use (policy [3225/4312/7320](#)), Internet Safety (policy [3226/4205](#)), Student Records (policy [4700](#)), Public Records – Retention, Release, and Disposition (policy [5070/7350](#)), Electronically Stored Information Retention (policy [5071/7351](#)), Employee Use of Social Media (policy [7335](#))

Adopted: December 16, 2019