BOARD MEMBER TECHNOLOGY USE

Policy Code: **2127**

A. BOARD MEMBER USE OF DISTRICT TECHNOLOGICAL RESOURCES

The Board provides its members with access to certain District technology devices and accounts, including laptops, tablets, phones and email accounts, for use in conducting District business. Board members have a responsibility to use such devices and accounts in a manner that is ethical, respectful, and supportive of the Board's duty to provide students with the opportunity to receive a sound, basic education. Like all users of District technological resources, Board members are expected to abide by the generally accepted rules of network etiquette.

1. Responsible Use of District Technological Resources

   Whenever a Board member uses District computers or other technology devices or accounts or accesses the school network or the Internet using District resources, the Board member must comply with the rules for use listed in Section B of policy 3225/4312/7320, Technology Responsible Use. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

2. Privacy Expectations when Using District Technological Resources

   Board members should have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the District's network, devices, Internet access, email system, or other technological resources owned or issued by the District, whether the resources are used on District property or elsewhere, and even if the use is for personal purposes. Files or communications created, transmitted, or displayed using District technological resources or stored on servers or on the storage mediums of individual devices will not necessarily be private. District personnel may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of medium, the content of electronic mailboxes, and system outputs, such as printouts, for any lawful purpose. Such purposes may include, but are not limited to, maintaining system integrity, security, or functionality, ensuring compliance with Board policy and applicable laws and regulations, protecting the District from liability, and complying with public records requests. District personnel may monitor online activities when the Internet is accessed via a District-owned device. By using the District's network, Internet access, email system, devices, or other technological resources, Board members consent to have that use monitored by authorized District personnel as described in this section.

B. BOARD MEMBER USE OF PERSONAL TECHNOLOGICAL RESOURCES FOR DISTRICT BUSINESS

As much as is practicable, Board members should use District technology devices for conducting District business and storing District electronically stored information ("ESI"). Though use of personal technology devices may be convenient for conducting District business, such use is discouraged when District resources are reasonably available. Board members may only use District accounts for conducting District Business. Only District-provided accounts and contact information will be published or shared.

1. Definition of Personal Technology Devices and Accounts

   For purposes of this policy, "personal technology devices and accounts" means technology devices or accounts that are not under the control of the District and which the District does not have the ability to access without the Board member's assistance. Personal technology devices include, but are not limited to, computers, phones, tablets, and other technological devices that are owned or leased by a Board member. Personal accounts include, but are not limited to, personal email accounts and online file storage services (e.g., file hosting services, cloud storage services, social media sites, and online file storage providers that host user files via the Internet). Board member use of personal social media sites is also subject to Section C of this policy.

2. District ESI on Personal Technology Devices and Accounts

   District business-related ESI sent and/or received by a Board member using a personal technology device or account may constitute a public record or student education record and, as a result, may require retention and disclosure by the District. In the event of litigation, District business-related ESI located on a personal technology device or account may be subject to discovery and a litigation hold. Board members are cautioned that using personal technology devices or accounts to conduct District business or to store District business-related ESI will significantly reduce their expectation of privacy in those devices or accounts. Board members should avoid the use of personal technology when conducting District business to prevent a conflict between Board members' interests in privacy in their personal technology devices and accounts and the District's legal obligation to preserve certain District business-related ESI.

   As the District is the custodian of public records, Board members are expected to immediately transfer, and may not delete, any District business-related ESI sent and/or received by the Board member using a personal technology device or account to a District account for proper retention and storage. If a Board member fails to immediately transfer all District business-related ESI, the individual Board member will be considered the custodian responsible for the maintenance of such records and will assume any and all associated liabilities. Board members shall cooperate with District officials in accessing any District business-related ESI stored on personal technology devices or accounts.

C. BOARD MEMBER USE OF PERSONAL SOCIAL MEDIA

The Board recognizes that Board members may engage in the use of personal social media to communicate with friends, family, and/or the community. Board members are expected to exercise good judgment in their online interactions, remaining mindful of their ethical obligations as described in policy 2120, Code of Ethics for School Board Members.

1. Definition of Personal Social Media

   For purposes of this policy, "personal social media" means any social media networks, tools, or activities that are not under the control of the District. Social media refers to the various online technology tools that enable people to communicate easily over the Internet to share information and resources. It includes, but is not limited to: personal websites, blogs, wikis, social networking sites, online forums, virtual worlds, video-sharing websites, and any other Internet-based applications which allow the exchange of user-generated content. Examples of social media include Web 2.0 tools, Facebook, X (formerly Twitter), LinkedIn, Flickr, YouTube, Instagram, and social media components of learning management systems such as Canvas, Moodle, or Edmodo.

2. Guidelines for All Types of Personal Social Media Use

   Content posted online may be viewed by anyone, including students, parents, employees, and community members. As public officials, Board members should be aware that their online behavior serves as an example to employees and students even when they are not engaging directly in District-related business. The following standards should guide Board members' online conduct.

   a. Board members should be professional in all Internet postings related to or referencing the District, students or their parents, and other employees.

   b. Board members may not post confidential information about students, employees, or District business.

   c. Board members should not post identifiable images of a student or student's family on a personal social media site without permission from the student and the student's parent or legal guardian.

   d. Board members may not use postings to libel or defame the Board, individual Board members, students, or individual District employees.

   e. Board members should not use personal social media to harass, bully, or intimidate students, employees, or other Board members.

   f. Board members may not use personal social media to engage in any other conduct that violates Board policy or administrative procedures or state and

federal laws.

3. Guidelines for Personal Social Media Use That Is District-Related

The District controls and maintains the District's official website, as well as the District's official Facebook, X and other social media accounts. The District website and social media accounts present information from the local school administrative unit and are not forums for expressing views of individual Board members, employees, or members of the public.

Individual Board members, acting in their capacity as public officials, may choose to establish personal social media accounts to facilitate their own communications with the community. The following standards are provided to guide Board members' personal social media use for District-related purposes.

a. When presenting information on personal social media, Board members should clearly indicate that the information posted reflects the views of the individual Board member and is neither endorsed by the Board nor necessarily reflective of the views of the Board or of an official Board policy.

b. A personal social media platform that allows comments from the community may elicit complaints or inquiries from parents or interested citizens concerning school matters. In such cases, the Board member should refer the complainant to the appropriate District administrator in accordance with policy 2015/5005 Constituent Services.

c. Board members are not authorized to speak on behalf of the Guilford County Board of Education or the Guilford County Schools on their personal social media accounts. Any statement made by an individual board member on a personal social media account reflects solely the personal views of that board member.

d. Board members may not use social media platforms to record or livestream during board meetings, retreats, work sessions, committee meetings or any other official gathering of the Board to conduct District business.

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; *Lindke v. Freed*, 601 U.S. __ (2024)

Cross References: Code of Ethics for School Board Members (policy 2120), , Constituent Services (policy 2015/5005), Technology Responsible Use (policy 3225/4312/7320), , Student Records (policy 4700), Public Records – Retention, Release, and Disposition (policy 5070/7350) Electronically Stored Information Retention (policy 5071/7351)

Adopted: June 1, 2021; TBD