PS-130
REV 9/2019

Sumter County Schools Computer Network Registration

PLEASE SELECT

☐ **NEW ACCOUNT** ☐ **CONTRACTOR/VENDOR** ☐ **CHANGES TO EXISTING ACCOUNT** [1]

☐ **REQUEST FOR A CLASS ACCOUNT W/ INTERNET** [2] ☐ **CLASS ACCOUNT W/O INTERNET** [2]

☐ **REQUEST FOR A GUEST STAFF ACCOUNT (for staff training or workgroups)**[3]

Please Print Using the Same Name as Your Human Resources Records Indicate

Last Name _____ **First Name** _____ **Middle Initial** _____

Site/School _____ **Position** _____ **EIN** (required for employees) _____

Contractors/Vendors: Please Indicate the Last Day of Services (or July 31 whichever is earlier) _____

[1] **For Name Changes, Please Indicate the Previous Name Below:**

_____

Option: Your primary email address will be based on your first and last name. If you are better known by a different name, we can set up a second "alias" with this name and in the directory:

_____

I have read and understand the Sumter County School District's **Staff Technology Acceptable Use And Safety** (Board Policy 7540.04) and agree to abide by the responsibilities therein.

I acknowledge that all software installed on my machine (downloaded or otherwise) must be properly licensed for use on that machine, and that I will adhere to the laws in respect to copyright. Users are responsible for maintaining proof of ownership for installed software excluding programs installed and licensed to the school or district.

I understand that most electronic mail messages through the district network may be public record and there should be no expectation of privacy or confidentiality. The district reserves the right to archive electronic correspondence. Notwithstanding the ability to archive, Media Services' role is similar to that of the U.S. Post Office. They provide an address to users, collect and deliver mail. Each individual is responsible for the appropriate retention or deletion of messages as related to applicable public records laws such as Florida's Sunshine Law.

I understand that the technology resources are operated for the expressed use to meet the mission and goals of the school district. The network must be protected from security risks that might impact the use or the protection of data within the network. Users are responsible to take precautions and immediately inform technical services if any breach of security is suspected.

I understand that as a public educational institution receiving federal funding, we must remain in compliance with the Children's Internet Protection Act. The Sumter District Schools have implemented technology measures to protect students from accessing inappropriate material on the Internet. Such measures are not infallible and the district requires proper supervision of students while using the Internet and no direct Internet based communication by students (chat, email) is permitted unless specific proper safeguards are in place. Any questions concerning these requirements are to be forwarded to the Media Services / Technology Department.

I understand that the security of the workstation and your user account resides with the user and that I am responsible for all activities performed under my user account. Users are responsible for the security of their passwords and should not provide it to any other individual. I understand my username and account is to be accessed only by the user. Computers are not to be left unattended while connected to a user account unless appropriate security measures, such as locking your workstation, have been implemented.

[2] **Class Accounts** are for the purpose of signing on student stations for ordinary activities so students do not have to log in or out individually. These are only to be used under the direct supervision of the staff member named. Password security is the responsibility of the staff member. The accounts may be with or without Internet Access. The responsibility for supervision remains with the named staff member.

[3] **Guest Staff Accounts** as indicated above are for the purpose of logging groups of adult users on to computers for training or workgroups. The rights of these accounts have certain permissions similar to staff members. Password security is the responsibility of the named staff member.

Applicant's Signature _____ **Date** _____

Administrator or Technology Approval _____ **Date** _____

APPROVED ☐	**---- District Media Services Department Use Only ----**	**DENIED** ☐
DATE CREATED:	☐ Name not verified	
EMAIL ADDRESS:	☐ Missing Information or Signature(s)	
	☐ Other:	

Staff Technology Acceptable Use and Safety 7540.04

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The School Board provides technology and information resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District's computer network and Internet system do not serve as a public access service or a public forum and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District technology and information resources by principles consistent with applicable local, State, and Federal laws and the District's educational mission. This policy and its related administrative procedures, Policy 7544 and any applicable employment contracts and collective bargaining agreements govern the staff's use of the District's technology and information resources and staff's wireless communication devices when they are connected to the District's computer network, Internet connection, and/or online educational services/apps, or when used while the staff member is on Board-owned property or at a Board-sponsored activity (see Policy 7530.02).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its technology resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District technology and information resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

Staff members are expected to utilize District technology and information resources to promote educational excellence in our schools by providing students with the opportunity to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services will be guided by Board Policy 2520 - Selection of and Adoption of Instructional Materials.

The Internet is a global information and communication network that brings incredible education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District technology resources provide students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

The Board may not be able to technologically limit access, through its technology resources, to only those services and resources that have been authorized for the purpose of instruction, study, and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act (CIPA). At the discretion of the Board or Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene,

objectionable, inappropriate, and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using the District technology resources if such disabling will cease to protect against access to materials that are prohibited under the CIPA. Any staff member who attempts to disable the technology protection measures without the express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

The Superintendent may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether the material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The Superintendent may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

Staff members will participate in professional development programs in accordance with the provisions of law and this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
B. the inherent danger of students disclosing personally identifiable information online;
C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students or staff online; and
D. unauthorized disclosure, use, and dissemination of personally identifiable information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above, and staff members will monitor students' online activities while at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying procedures. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the District technology resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including in chat rooms and cyberbullying awareness and response. All users of District technology resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying procedures.

Staff will be assigned a school email address that they are required to utilize for all school-related electronic communications, including those to students, parents and other constituents, fellow staff members, and vendors or individuals seeking to do business with the District.

With prior approval from the Superintendent, staff may direct students who have been issued school-assigned email accounts to use those accounts when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the students for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District technology and information resources - i.e., behavior comparable to that expected when they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of its technology and information resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying procedures and Policy 7544 and its accompanying procedure.

Staff members use of District technology resources to access or use social media is to be consistent with Policy 7544 and its accompanying procedure.

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

General school rules for behavior and communication apply.

Users who disregard this policy and its accompanying procedures may have their use privileges suspended or revoked and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District technology and information resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent as the administrator responsible for initiating, implementing, and enforcing this policy and its accompanying procedures as they apply to staff members' use of District technology and information resources.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent (see Policy 8330). Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential student or employee information may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.