



**Sumter County Schools**

**Computer Network Registration**

**PLEASE SELECT**

- NEW ACCOUNT                       CONTRACTOR/VENDOR                       CHANGES TO EXISTING ACCOUNT <sup>1</sup>
- REQUEST FOR A CLASS ACCOUNT W/ INTERNET <sup>2</sup>                       CLASS ACCOUNT W/O INTERNET <sup>2</sup>
- REQUEST FOR A GUEST STAFF ACCOUNT (for staff training or workgroups)<sup>3</sup>

**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) \_\_\_\_\_

<sup>1</sup> 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 Technology Resources Acceptable Use Policy (Board Policy 8.62) 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.

<sup>2</sup> **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.

<sup>3</sup> **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 <input type="checkbox"/> |  | --- District Media Services Department Use Only ---          |  | DENIED <input type="checkbox"/> |  |
| DATE CREATED:                     |  | <input type="checkbox"/> Name not verified                   |  |                                 |  |
| EMAIL ADDRESS:                    |  | <input type="checkbox"/> Missing Information or Signature(s) |  |                                 |  |
|                                   |  | <input type="checkbox"/> Other:                              |  |                                 |  |
|                                   |  |  |  |                                 |  |
|                                   |  |  |  |                                 |  |

The data network system of the District is available for use by employees and students of the District in order to provide them with equal access to the computing resources which serve public education. The data network system is an electronic highway that connects thousands of computers all over the world and millions of individual subscribers. All personnel having authorization to use the network will have access to a variety of information sources. The District's technological resources are components of the data network system. This policy is in effect whether the district owned resource is connected to the district network or in use outside the network.

- I. The use of these technology resources is a privilege, not a right.
- II. No expectation of privacy or confidentiality in the content of electronic communications including, but not limited to, computer files, electronic messaging, facsimile or other transmissions sent, received through or stored on the communication resources of the Sumter District Schools should be expected by users. Such information is subject to review, monitoring and archiving. The District reserves the right to remove them and report any violation of rules to school and/or District administration and/or law enforcement. For the safety and security of students, District supported electronic communications for students will be monitored and filtered.
- III. Access to material on the worldwide interconnected network, does not provide for the use of the same selection procedures as the School District follows in regard to other instructional materials, such as textbooks. Similar to broadcast and other current event media, the material available is vast and ever changing. With such access, comes the potential availability of material that may be harmful to minors or not be considered to be of educational value in the context of the school setting. Specifically, the District supports those which will enhance the research and inquiry of the learner with directed guidance from faculty and staff. At each school, each student's access to use the network will be under the teacher's direction and monitored as a regular instructional activity.
- IV. The District will maintain technology protection measures to limit student's access to prohibited material. While the District uses Internet content filters, any filtering of information should not be considered all inclusive. The District cannot prevent the possibility that some users may access material that is not consistent with the educational mission, goals and policies of the District. This is particularly possible since access to the Internet may be obtained at sites other than school or on devices outside the authority of the school. The Sumter District Schools reserves the right to limit the content of material students access due to legitimate pedagogical, safety and system integrity concerns.
- V. At each school and facility owned or operated by the District, notices shall be conspicuously posted that state the following:

"Users of the data network system of the Sumter County School District are responsible for their activity on the network. The School District has developed a technology resources acceptable use policy. All users of the network are bound by that policy. Any violation of the policy may result in the suspension of access privileges or other disciplinary action, including student expulsion and employee dismissal."

- VI. The use of the network and technological tools shall be consistent with the mission, goals, policies, and priorities of the District. Successful participation in the network requires that its users regard it as a shared resource and that members conduct themselves in a responsible, ethical and legal manner while using the network. Any use of the network or technological tools for illegal, inappropriate or obscene purposes, or in support of such activities, will not be tolerated. Examples of unacceptable uses of the network or technological tools include, but are not limited to:
  - A. Violating the conditions of the Education Code dealing with student's rights to privacy;
  - B. Using, transmitting or accessing profane, obscene, lewd/indecent (which includes what is commonly referred to as sexting) or other materials harmful to minors;
  - C. Copying commercial software or other content in violation of copyright law or other copyright protected material;
  - D. Using the network or technological tools for financial gain or for any commercial or illegal activity;
  - E. Using the network or technological tools for the advancement or disparagement of any particular candidate or political party;
  - F. Taking any actions that affect the ability of the District to retrieve or retain a record of any use of the computer equipment or data network system, including but not limited to, adding or modifying the existing software without specific permission; creating, uploading and/or intentionally accessing computer viruses or material blocked by the District's technology protection measures; intentional damage to technological equipment or any other action for the purpose of limiting the usability of the network or technological tools.
  - G. Taking any actions that affect other students' ability to use the technological resources, including but not limited to, vandalism or "hacking".
  - H. Transmitting student identifying information over the data network system, except as part of the approved educational program as permitted by law; and
  - I. Other actions that are not in accordance with the *Code of Ethics* and *Principles of Professional Conduct of the Education Professional of Florida* for staff and *The Code of Student Conduct* for students.
- VII. Schools and Departments in the Sumter School District may have additional guidelines for appropriate use. These policies will be developed and enforced in consort with this District policy.
- VIII. Schools are required to educate their students about appropriate online behaviors including but not limited to interactions with other individuals through communication methods or social networking. Instruction will include cyber bullying awareness and response.
- IX. The District recognizes the use of social media for communication and e-learning; however, only those networks sponsored by the District may be used for classroom instruction or school sponsored activities without the approval of the Superintendent or his designee.
- X. Failure to adhere to this policy may result in suspending or revoking the offender's privilege of access to the network and other disciplinary action up to and including, termination of the employee or expulsion in the case of a student, and possible criminal prosecution if applicable. Any possible illegal acts discovered by students or employees shall be reported to the appropriate legal authority.
- XI. Any student shall be exempt from instruction on accessing the data network upon request in writing from the parents, as defined by Florida Statutes, to the principal. The request for exemption shall expire at the end of each school year. It shall be the responsibility of the parent to renew the request yearly.

**STATUTORY AUTHORITY:**  
**LAW(S) IMPLEMENTED:**  
**HISTORY:**

**1001.41, 1001.42, F.S.**  
**1000.21, 1001.43, F.S.**  
**ADOPTED: 11/16/2004**  
**REVISION DATE(S): 3/7/2006, 8/7/2007, 4/3/12, 7/24/2012**  
**FORMERLY: 2.52**