

Wa-Nee Community Schools

# Staff Network and Internet Acceptable Use and Safety



*Leading Education And Progress*  
Merging the Past, Present, and Future of Learning

## STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

Advances in telecommunications and other related technologies have fundamentally altered the ways in which information is accessed, communicated, and transferred in our society. Such changes are driving the need for educators to adapt their means and methods of instruction, and the way they approach student learning, to harness and utilize the vast, diverse, and unique resources available on the Internet.

The School Board is pleased to provide Internet services to its staff. The Corporation's Internet system is limited to educational purposes. The Corporation's Internet system has not been established as a public access service or a public forum. The Corporation has the right to place restrictions on its use to assure that use of the Corporation's Internet system is in accord with its educational purpose. Staff use of the Corporation's computers, network and Internet services ("Network") will be governed by this policy and the related administrative guidelines, and any applicable employment contracts and collective bargaining agreements. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Network. Users have a limited expectation of privacy in the content of their personal files and records of their online activity while on the Network.

The Corporation encourages staff to utilize the Internet in order to promote educational excellence in our schools by providing them 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 will be guided by the Corporation's policy on instructional materials.

The Internet is a global information and communication network that provides students and staff with access to up-to-date, highly relevant information that will enhance their learning and the education process. Further, the Internet provides 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 certain unique challenges and responsibilities.

First, and foremost, the Corporation may not be able to technologically limit access, to services through the Corporation's Internet connection, to only those 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, will open classrooms and students to electronic information resources which have not been screened by educators for use by students of various ages.

The Corporation has implemented the use of technology protection measures which are specific technologies that will protect against (e.g. filter or block) access to visual displays/depictions that are obscene, child pornography, and materials that are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Corporation or the Superintendent, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The technology protection measures may not be disabled at any time that students may be using the Network, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection act. Any staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

The Superintendent or Director of Technology may temporarily or permanently unblock access to sites containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether 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 or Director of Technology may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

The Corporation has implemented technology protection measures which block/filter Internet access to visual displays that are obscene, child pornography or harmful to minors. The Corporation 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 Superintendent or Director of Technology may 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. safety and security of students while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
- B. the inherent dangers of students disclosing personally identifiable information online; and,
- C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by students online; and

D. unauthorized disclosure, use, and dissemination of personal 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 the online activities of students 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 guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the Internet. All Internet users are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines. Staff members are responsible for good behavior on the Corporation's computers/network and the Internet just as they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature.

Staff members shall not access social media for personal use from the Corporation's network, and shall access social media for educational use only after submitting a plan for that educational use and securing the principal's approval of that plan in advance. General school rules for behavior and communication apply. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines. Users who disregard this policy and its accompanying guidelines may have their user privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the Internet through the district's computers assume personal responsibility and liability, both civil and criminal, for use of the Internet not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and the Director of Technology as the administrator responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of the Network.

### **Social Media Use**

An employee's personal or private use of social media, such as Facebook, Twitter, MySpace, blog, etc., 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 Corporation'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.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parent 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.

P.L. 106-554 (2000), Children's Internet Protection Act

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

20 U.S.C. 6777, 9134 (2003)