Instruction

Access to Electronic Networks

The School is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the School will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum

The use of the School's electronic networks shall: (1) be consistent with the curriculum adopted by the School as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library-media center materials. Staff members may, consistent with the Principal's implementation plan, use the Internet throughout the curriculum.

The School's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the School's electronic network must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the School's electronic network or School computers. General rules for behavior and communications apply when using electronic networks. The School's *Authorization for Electronic Network Access* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Each School computer with Internet access shall have a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Principal or designee. The Principal or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Principal or system administrator.

The Principal or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks;
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials;
3. Ensure student and staff privacy, safety, and security when using electronic communications;
4. Restrict unauthorized access, including "hacking" and other unlawful activities; and

5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each staff member must sign the School's *Authorization for Electronic Network Access* as a condition for using the School's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use.

All users of the School's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

The failure of any student or staff member to follow the terms of the *Authorization for Electronic Network Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Approved: 11/8/11