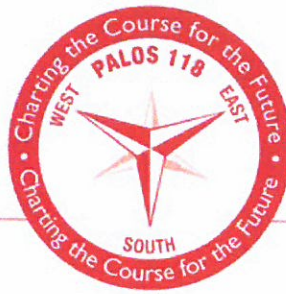


PALOS



118

PALOS COMMUNITY CONSOLIDATED SCHOOL DISTRICT 118

Dear Parents:

Attached you will find our Network Usage policy. Our policy is based on a model provided by the Illinois Association of School Boards and provides guidelines that include respect for intellectual property and copyright as well as network etiquette and safety. All students receive an age appropriate overview of the rules and responsibilities for use of our network at school, but we encourage you to go over the main points with your children and take this opportunity to address your own expectations for their use of digital tools at home as well as at school. We believe that clear expectations of safe and responsible online behavior combined with adult supervision are the most important safeguards we can provide.

District 118 has made a significant commitment to technology and digital content to support student learning. Many high quality and relevant instructional materials are available on the Internet, including content and updates from publishers of textbooks used in our schools. Teachers may select online resources for use with their classes just as they choose text and other media sources to support instruction. Students are not provided e-mail accounts; any class projects involving e-mail utilize teacher accounts only.

Sincerely,

A handwritten signature in black ink, appearing to read "Anthony M. Scarsella". The signature is fluid and cursive, with a long horizontal stroke at the end.

Anthony M. Scarsella
Superintendent of Schools

Instruction

Access to Electronic Networks

Electronic networks, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent or designee shall develop an implementation plan for this policy and appoint a 'system administrator'. This policy shall apply to all use of the District's computers.

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

Curriculum and Appropriate Online Behavior

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District 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 resource center materials. As required by federal law and Board policy 6:60, *Curriculum Content*, students will be educated about appropriate online behavior, including but not limited to: (1) interacting with other individuals on social networking websites and in chat rooms, and (2) cyber-bullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

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

Acceptable Use

All use of the District's electronic network must be in support of education and/or research, and be in furtherance of the School Board's stated goal, or for a legitimate school business purpose. Use is a privilege, not a right. The District's electronic network and computers, including all software and equipment, is the property of the District. The District may monitor any and all computers to determine, among other things, the websites that any user has visited or attempted to visit, e-mail communications made or received, data or material stored in any computer, or for any other purpose. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic network or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic Network Access* attached as an Exhibit to this Policy and made a part of this Policy contains the appropriate uses, ethics, and protocol. Electronic communications, files, data and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials at any time, with or without cause and with or without notice.

Internet Safety

Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The Superintendent 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. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials;

2. Student safety and security when using electronic communications;
3. Limiting unauthorized access, including “hacking” and other unlawful activities; and
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Authorization for Electronic Network Access

Each staff member must sign the District's *Authorization for Electronic Network Access* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use. The Authorization is attached as an Exhibit to this Policy and is made a part of this Policy.

All users of the District’s computers and means of Internet access 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, up to and including suspension and/or expulsion or, in the case of employees, termination and/or appropriate legal action.

- LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.
 Children’s Internet Protection Act, 47 U.S.C. §254(h) and (l).
 Enhancing Education Through Technology Act, 20 U.S.C §6751 *et seq.*
 47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
 720 ILCS 135/0.01.
- CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright for Publication or Sale of Instructional Materials and Computer Programs Developed by Employees), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials), 6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Publications)
- ADMIN PROC.: 6:235-AP (Administrative Procedure - Acceptable Use of Electronic Networks), 6:235-E2 (Exhibit - Authorization for Electronic Network Access)
- ADOPTED: August 14, 2012