# NETWORK ACCEPTABLE USE 8.60+

I. The network system of the District is available for all employees and students of the District in order to provide them with equal access to the computing resources which serve public education. The network system is an electronic highway which connects thousands of computers all over the world and millions of individual subscribers. The term *network* may include electronic mail, worldwide Web browsing, or any method of connecting with other computer equipment. All personnel having authorization to use the network will have access to a variety of information.

II. Some material on the network might not be considered to be of educational value in the context of the school setting. In addition, some material, individual contacts, or communications may not be suitable for school-aged children. The District views information retrieval from the network in the same capacity as information retrieval from reference materials identified by schools. Specifically, the District supports information retrieval from the network which enhances the research and inquiry of the learner and which faculty and staff direct. The District network will filter inappropriate material. At each school, each student's access to use of the network will be under the teacher's direction and monitored as a regular instructional activity.

III. 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 network may be obtained at sites other than school.

IV. At each school and facility owned or operated by the District, in each room where computers are present, notices shall be conspicuously posted that state the following:

> Users of the network system of the School District of Osceola County are responsible for their activity on the network. The School District has developed a data network acceptable use policy. All users of the network are bound by that policy. Any violation of the policy will result in the suspension of access privileges or other disciplinary action, including student expulsion and employee dismissal. This notice shall also become part of the login process.

V. The use of the network 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 for illegal, inappropriate, or obscene purposes, or in support of such activities, will not be tolerated. For compliance with the requirements of the Elementary and Secondary Education Act (ESEA) and the Children's Internet Protection Act (CIPA), please see procedures entitled "Student Internet Use Procedures."

Examples of unacceptable uses of the network include, but are not limited to:

1. Violating the conditions of The Code of Ethics and Principles of Profess ional Conduct of the Education Profession of Florida dealing with student's rights to privacy, employee rights to privacy, or violating any other section of the Code;

2. Using, accessing, visiting, downloading, or transmitting inappropriate material, messages or images such as pornography, profanity or obscenity;

3. Reposting personal communications without the author's consent;

4. Copying, sending (uploading) or receiving (downloading) commercial software in violation of copyright law or other copyright protection of trademarked material;

5. Using the network for financial gain or for any commercial or illegal activity;

6. Using the network for political advertisement or political activity;

7. Taking any actions that affect the ability of the District to retrieve or retain any information contained on the computer equipment, in the data network system or acting to modify any software or any data without specific written permission;

8. Sending any student identifying information, via e-mail, over the network system, may be done only when the sender and receiver are members of the District's FirstClass e-mail. FirstClass e-mail is encrypted to protect the confidentiality of the message. E-mail containing confidential student information must adhere to the *District's E-Mail and Student Confidentiality* policy;

9. Creating and/or forwarding advertisements chain letters, mass mailings, get rich quick schemes, and pyramid schemes to individual mailboxes

and/or mailing lists;

10. Gambling or conducting any illegal activity;

11. Posting personal views on social, political, religious or other nonbusiness related matters;

12. Creating and/or forwarding messages, jokes, etc., which violate School Board harassment policies and/or create an intimidating or hostile environment.

VI. The e-mail system and the hardware are owned by the District and are intended for District business use. Minor personal use of e-mail and the internet by school district employees is acceptable, but should not interfere or conflict with District business.

VII. District business conducted by e-mail must be done using the e-mail account that the district supplies. When an employee conducts official business of the District via e-mail, the employee must retain a copy of the e-mail including attachments in paper form or store these documents electronically on district owned equipment in accordance with the Florida Public Records law and the District Records Management Manual.

VIII. 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.

IX. Any student shall be exempt from accessing the internet 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.

X. The District reserves the right to monitor and/or retrieve the contents of e-mail messages for legitimate reasons such as, but not limited to, ensuring the integrity of the system, complying with investigations of wrongful acts, or recovering from a system failure.

XI. District employees' and students' passwords are confidential, and in order to maintain network security, employees/ students shall:

A. Change passwords at least four (4) times a year, or whenever the employee feels his/her password may have been compromised;

B. Use passwords that contain letters and numbers and that are difficult to guess, or

C. Type in passwords at each log in.

D. Employees shall not share passwords and shall not set passwords to an automatic log in mode.

E. It may become necessary to know employee or student passwords for maintenance purposes. Only authorized computer maintenance personnel will be allowed to know passwords. Upon completion of the maintenance activity, the user will need to change their password.

XII. All Web sites representing any District employee pursuant to their official District role and duties must have their Web site hosted on a school district file server. File server space, Web site design software, and technical assistance are provided to school district employees to facilitate posting of District business-related Web pages. Using free or paid outside Web servers for public dissemination of District business is not permitted.

**STATUTORY AUTHORITY:** **1001.41, 1001.42, F.S.**

**LAW(S) IMPLEMENTED:** **1000.21, 1001.43, F.S.**

**HISTORY:** **REVISION(S): 12/06/05, 05/01/07, 02/05/08, 10/21/08, 08/25/09, 07/13/10**

**FORMERLY: 3.21**