

**POLICY 6111****DOWNERS GROVE GRADE SCHOOL DISTRICT 58****INSTRUCTION**Computer Network and Internet Safety, Access and Use

This Policy and its implementing Administrative Regulations are intended to define the scope of the District's authority, and the safe and acceptable use of the District's computers, computer network, and Internet access. This Policy governs all use of District computers, the District's local and/or wide area network, and access to the Internet through District computers or the District's local and/or wide area network, which will be collectively referred to in this Policy and its implementing Administrative Regulations as the District's "computer network."

**I. Access to Network**

Access to the District computer network is consistent with the educational mission of the District. Such access serves as a natural extension of classroom learning by providing access to educational resources and reference materials, by reinforcing the specific subject matter taught, by requiring the use of critical thinking skills, by promoting tolerance for diverse views, and by teaching socially appropriate forms of civil discourse and expression. Therefore, students, teachers, administrators, other employees of the District, and Board of Education members shall be allowed access to the District computer network consistent with the District's curriculum, educational mission and this Policy and its implementing Administrative Regulations.

**II. Use of Network**

The District 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.

The District's computer network is part of the curriculum and is not intended to be used as a public forum for general use. Access to the computer network 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 District's electronic networks or District computers. The Board of Education has a duty to insure that the manner in which the computer network is used does not conflict with the educational mission of the District. Use of the District's computer network may be restricted in light of the maturity level of students involved and the special

characteristics of the school environment. Therefore, the District shall not permit use of the computer network which:

- (a) disrupts the proper and orderly operation and discipline of schools in the District;
- (b) threatens the integrity or efficient operation of the District's computer network;
- (c) violates the rights of others;
- (d) is socially inappropriate or inappropriate for a student's age or maturity level;
- (e) is primarily intended for commercial use or as an immediate solicitation of funds;
- (f) is illegal or for illegal purposes of any kind;
- (g) constitutes gross disobedience or misconduct; or
- (h) results in unauthorized charges or fees to the District.

### III. Internet Safety

The District shall also implement technology protection measures consistent with the *Children's Internet Protection Act* and its implementing regulations.

Each District 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 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 during use by non-student adults for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator.

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.

#### IV. Implementation/Compliance

The Superintendent and Building Principals are authorized to implement this Policy and its Administrative Regulations, and to designate appropriate staff members to assist them in doing so. The District shall monitor the use of the computer network by students and any other minor users in order to ensure compliance with the Policy and related Administrative Regulations. The Superintendent and Building Principals may also promulgate additional rules, regulations, and other terms and conditions of computer network use as may be necessary to ensure the safe, proper, and efficient operation of the computer network and the individual District schools.

Legal Reference: 18 U.S.C. § 2511  
20 U.S.C. § 7001  
47 U.S.C. § 254(h)

Adopted: 05/12/97  
Reviewed: 02/27/01  
Revised: 07/14/03  
Revised: 05/14/07  
Revised: 07/12/10