TECHNOLOGY RESOURCES AND ACCESS TO ELECTRONIC NETWORKS

Goal and Acceptable Use

The District 89 Board of Education encourages the responsible use of technology resources to facilitate the instructional program and to promote resource sharing, communication, innovation and research. All access of the District's technology resources shall reflect this intent and shall be considered a privilege rather than a right. The District's technology resources are intended for curricular use and shall not be a public forum for general use.

District Technology Resources

Technology resources within District 89 shall include all information accessed by, but not limited to, computer systems (host computers, file servers, workstations, printers, scanners, standalone computers, laptops, software, etc.), audio/visual equipment (LCD Projectors, DVD players, televisions, scan converters, digital cameras, document cameras, Interactive White Board, etc.), communications equipment (telephones, fax machines, etc.), and internal or external communications networks (Internet, commercial online services, and electronic mail systems), and all mobile telecommunication devices, including but not limited to, mobile or cellular telephones, tablets, e-readers, mp3 players, and any other hand-held device that has the capability of transferring data or voice, that are accessed directly or indirectly from the technology facilities provided by CCSD 89.

Rules and Responsibility for Access

All policies and regulations applicable to behavior and communications shall apply to the use of technology resources. The District's "Authorization for Technology Access" shall provide an explanation of the appropriate uses, ethics, and protocol. Specific rules governing the use of technology resources shall be delineated in Regulation 600:235-R. Students and staff should have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic network, District computers, or other District electronic devices. Electronic communications and downloaded material may be monitored or read by school officials. All use of the District's electronic network, computers, or other electronic devices must be for a legitimate school business purpose or in support of education and/or research, and be in furtherance of the goals stated herein.

The District's "Student's Authorization for Telecommunication Network Access" (600:235-F1) must be signed before a student shall be granted unsupervised use. This document will be signed by the parent(s)/guardian(s) for children up through second grade. Students must be provided with an explanation of the District's acceptable use of technology and complete the form in grades 3 and 6. This information will be reviewed with students on an annual basis. All new students and/or their parent(s)/guardian(s) shall sign form 600:235-F1 upon enrollment. District 89 employees and Board members must also sign the District's "Teacher and Non-Student Authorization for Telecommunication Network Access" (600:235-F3) as a condition for use. 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.

The failure of any student or educator to follow the terms of the "Authorization for Technology Access" or this policy will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Internet Safety

Each District digital device with Internet access shall have a filtering device designed to block entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by state and federal law and as determined by the Superintendent. The Superintendent 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 Superintendent or system administrator. The Superintendent 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, including the safe and responsible use of social networking websites, chat rooms, electronic mail, bulletin boards, instant messaging, and other means of communication on the Internet. Student safety shall also address recognizing, avoiding, and reporting online solicitations of students, their classmates, and their friends by sexual predators, limiting risks by not transmitting personal information on the Internet, recognizing and avoiding unsolicited or deceptive communications received online, recognizing and reporting online harassment and cyber- bullying, recognizing and reporting illegal Internet activities and communications.
3. Limiting unauthorized access, including "hacking" and other unlawful activities;
4. Teaching students about copyright laws in regard to written materials, photographs, music and video; and
5. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Network Etiquette

The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

1. Be polite. Do not become abusive in messages or interactions with others;
2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language;
3. Do not reveal personal information, including the addresses or telephone numbers of students or colleagues;
4. **Recognize that email is not private.** People who operate the system have access to all email. Messages relating to or in support of illegal activities will be reported to the authorities and may result in discipline;
5 Do not use the network in any way that would disrupt its use by other users;
6. Consider all communications and information on District computers and the network accessible by the District.

District and School Websites

Pictures of CCSD89 students and exemplary work, accompanied by a student's first name and last initial, may be published on District and school websites, unless a parent withholds consent by signing form 600:235-F4, "Student Publication Authorization".

CROSS REF: Policy 400:19 (Employee Interaction with Students); Regulation 600:235-R; Forms 600:235-F1 to 600:235-F4, and 600:235-E

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).
Enhances Education Through Technology, 20 U.S.C §6751 et seq.
720 ILCS 5/11 et seq.

POLICY

Adopted: 8/17/98
Revised: 7/17/06, 6/18/07, 5/18/09, 11/14/11, 7/21/14, 11/17/14, 6/15/15, 12/18/17
Reviewed: 5/14/18, 5/20/19

COMMUNITY CONSOLIDATED SCHOOL DISTRICT 89
Learning for Life

Board of Education, Glen Ellyn, Illinois