

6:235 Access to Electronic Networks

Electronic networks, including the Internet, are a part of KASEC's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The Executive Director shall develop an implementation plan for this policy and appoint system administrator(s).

KASEC 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, KASEC will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior

The use of KASEC's electronic networks shall: (1) be consistent with the curriculum adopted by KASEC 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. Staff members may, consistent with the Executive Director's implementation plan, use the Internet throughout the curriculum.

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

Acceptable Use

All use of KASEC's electronic networks 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 KASEC's electronic networks or KASEC computers. General rules for behavior and communications apply when using electronic networks. KASEC's administrative procedure, *Acceptable Use of KASEC's Electronic Networks*, 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

Technology protection measures shall be used on each KASEC 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 federal law and as determined by the Director or designee. The Director 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 Director or system administrator. The Director 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 *Authorization for Access to KASEC's Electronic Networks* as a condition for using KASEC'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 KASEC'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 KASEC's administrative procedure, *Acceptable Use of KASEC's Electronic Networks*, or this policy, will result in the loss of privileges, disciplinary action, 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 5/26.5.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:210 (Instructional Materials), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Behavior), 7:310 (Restrictions on Publications; Elementary Schools)

ADOPTED: November 14, 2019