

REGIONAL SCHOOL UNIT #38
STUDENT COMPUTER, INTERNET USE, AND CYBER SAFETY

It is the policy of Regional School Unit #38 (RSU #38) to: a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; b) prevent unauthorized access and other unlawful online activity; c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

RSU #38's computers, networks and Internet access are provided to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. This policy and the accompanying rules also apply to laptops/tablets issued directly to students, whether in use at school or off school premises. Students are not allowed to use privately owned laptops/tablets at school. A privately owned laptop/tablet brought to school without authorization may be confiscated.

Student use of school computers, networks, Internet services, and email is a privilege, not a right. Compliance with the school unit's policies and rules concerning computer and Internet use is mandatory. Students who violate these policies and rules may have their computer privileges limited, suspended, or revoked. Such violations may also result in disciplinary action, referral to law enforcement and/or legal action. All students will adhere to the copyright provisions of Policy EGAD, Copyright Compliance. Students are prohibited from using school computers in any manner that would be in violation of the district Policy on harassment.

RSU #38 computers remain under the control, custody and supervision of the school unit at all times. The school unit monitors all computer and Internet activity by students. The school unit may conduct random audits of computer usage to protect its technology infrastructure. RSU #38 has the right to access, review and/or disclose any aspect of computer usage when it has legitimate business or security need to do so. Students have no expectation of privacy in their use of school computers, whether they are used on school property or elsewhere.

The RSU #38 utilizes filtering technology designed to block materials that are illegal, obscene or harmful to minors, including all pornography. RSU #38 takes precautions to supervise student use of the Internet and electronic communications, and to prevent unlawful disclosure, use or dissemination of personally identifiable information about students. RSU #38 educates students about safety on the Internet, appropriate online behavior and cyberbullying awareness and response, but parents should be aware that RSU #38 cannot reasonably prevent all instances of inappropriate computer and Internet use by students in violation of Board policies and rules, including access to objectionable materials and communication with persons outside of the school. The school unit is not responsible for the accuracy or quality of information that students obtain through the Internet.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: a) unauthorized access, including so-called "hacking", and other unlawful activities; and b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

The Superintendent is responsible for implementing this policy and the accompanying rules and for documenting student Internet safety training. Additional administrative procedures or school rules governing the day-to-day management and operations of the school unit's computer system may be implemented, consistent with Board policies and rules. The Superintendent may delegate specific responsibilities to the technology director and others as he/she deems appropriate.

Students and parents shall be informed of this policy and the accompanying rules through handbooks, the school web site and/or other means selected by the Superintendent.

Students and their parent/guardian are required to sign and return the Computer/Internet Access Acknowledgment Form (IJNDB-E) before being allowed to use school computers.

Cross Reference: ACAA, Harassment and Sexual Harassment of Students
 ACAB, Harassment and Sexual Harassment of School Employees
 EGAD, Copyright Compliance
 GCSA, Employee Computer and Internet Use
 IJNDA, Distance Learning Program
 IJNDB-E1, Electronic Resources – User Acknowledgment Form (student)
 IJNDB-E2, Electronic Resources – User Acknowledgment Form (parent)
 IJNDB-R, Student Computer and Internet Use Rules
 JIC, Student Code of Conduct
 JICJ, Student Use of Cell Phones and Other Electronic Devices
 JICJ-R, Student Use of Cell Phones and Other Electronic Devices Procedures

Legal Reference: 47 USC § 254(h)(5) (Children's Internet Protection Act)

Adopted: 06/01/06

Adopted by RSU #38 Board of Directors: 04/27/09

Revised by RSU #38 Board of Directors: 12/4/13

Revised Date: 06/01/16