STUDENT COMPUTING DEVICE AND INTERNET USE

RSU #34's computing devices, network, and internet access are provided to support the educational mission of the schools. This policy and the accompanying rules also apply to computing devices issued directly to students, whether in use at school or off school premises. Students are allowed to use privately-owned computing devices at school with prior authorization, provided that they comply with this policy and the accompanying rules.

The phrase "computing device" as used in this policy and subsequent rules refers to all computing devices, including but not limited to desktops, laptops, tablets, and smartphones.

Compliance with the school unit's policies and rules concerning device, network, and internet use is mandatory. Students who violate these policies and rules may, after being given an opportunity to respond to an alleged violation, have their computing device privileges limited, suspended, or revoked. The building administrator shall have the final authority to decide whether a student's privileges will be altered, based on the circumstances of the particular case. Such violations may also result in disciplinary action, referral to law enforcement, and/or legal action.

RSU #34 computing devices are at all times subject to the control, custody, and supervision of the school unit. The school unit may monitor all computing device and internet activity by students. Students have no expectation of privacy in their use of school computing devices, whether they are used on or off school property. This does not guarantee that student activities on RSU #34 computing devices are actively monitored 24 hours per day.

For computing devices not owned by RSU #34, students have no expectation of privacy for use that occurs in RSU #34 buildings, on the RSU #34 network, or through RSU #34 electronic media (e.g., google apps, server-based applications). This does not guarantee that student activities on RSU #34 networks or media are actively monitored 24 hours per day.

Disciplinary action can occur for events on or off campus, if such events make use of RSU #34 computing devices, network, or electronic media.

RSU #34 utilizes filtering technology designed to block materials that are obscene or harmful to minors and child pornography while connected to the district network. RSU #34 takes precautions to supervise student use of the internet and electronic communications, and to prevent the unlawful disclosure, use, or dissemination of personally identifiable information about students. RSU #34 educates students about safety on the internet, appropriate online behavior, and cyber-bullying awareness and response, but parents should be aware that RSU #34 cannot reasonably prevent all instances of inappropriate use by students that may violate Board policies and rules, including access to objectionable materials and communications.

RSU #34 uses a number of network-based services for purposes related to the mission and management of schools, such as data management, student assessment, and learning

assistance. Prior to choosing software and services, RSU #34 staff, guided by the RSU #34 Technology Committee and the IT department, shall give due consideration to the relative risks and rewards (e.g., consideration of privacy risks relative to the educational gains from a network-based account). Students shall generally be given unique passwords to accounts that contain information that could be used to gain a child's trust (e.g., profiles, interests). If a generic password is used (for example, with younger students) such accounts would be made available only within the school network.

RSU #34 staff will make reasonable efforts to promptly make parents/guardians aware of network-based or internet-based accounts used by their child in the school setting. Upon parent/guardian request, a staff member (usually the teacher implementing the system) will meet to describe the account purpose and use, and to show the parent/guardian their child's login. At such meeting, the parent/guardian should be provided with their child's login and password upon request.

Parents/guardians may request to exclude their student from use of some network-based services (examples of exceptions include the Student Information System, mandated online state assessments, and data management systems). Such requests should be made initially to the educator implementing the system; either the parent/guardian or educator may choose to involve the building administrator or other appropriate staff in this consideration.

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

The Superintendent or his/her designee is responsible for implementing this policy and the accompanying rules. Additional administrative procedures or school rules governing the day-to-day management and operations of the school unit's devices, network, and internet access may be implemented by the Superintendent, consistent with Board policies and rules.

Cross Reference:

IJNDB-R Student Computing Device and Internet Use Rules
JICIA - Weapons, Violence, Bullying and School Safety
GBEB - Staff Conduct with Students
GCSA/GCSA-R - Employee Computing Device and Internet Use

Legal Reference
47 USC 254(h)(5) (Chíldren's Internet Protection Act)
P.L. No. 110-385 (Protecting Children in the 21st Century Act)

First Reading: July 17, 2013
Adopted: August 21, 2013