Student Internet and Computer Use Policy

Purpose and Scope

Access to information is a fundamental right in a democratic society. For that reason, the [X School District] makes every effort to provide students and faculty with advanced information technologies. The internet offers our community broad access to information and opportunities for communication and learning. At the same time, student internet use presents new challenges for our school community. This policy aims to strike a balance between open access and safety, to ensure students have the freedom to intellectually explore and grow in a productive and healthy environment.

This policy governs information created, stored, sent, and received on campus internet networks (including wifi), district-owned computers and other internet connected devices (including student-owned or other personal devices), and district-provided computer programs and software, including student email and educational apps. It sets out expectations for responsible student internet and computer use, establishes disciplinary guidelines to address policy violations, and provides clear guidance to students about their rights to digital privacy. For school policy governing student-owned electronic devices at school, see XXXXXX.

In order to use the school network or internet connected devices at school, students and their parents must read and sign this acceptable use policy. Due to the ever-evolving nature of technological systems and platforms, this policy will be reviewed each year and modified as needed on an annual basis.

Acceptable and Prohibited Uses of School Networks, Technologies, and Devices

Students are encouraged to use school networks, technologies, and devices:

- to complete school assignments;
- to research school projects;
- to communicate with teachers, administrators, coaches, and other students about educational and extracurricular matters;
- at the direction of teachers, administrators, or other school officials; and
- in a manner that comports with other school policies.

Students shall not use the school network or school technologies to:

- intimidate, harass, threaten, or bully anyone;
- post their or others' personal information online, including but not limited to date of birth, social security number, address, telephone number, credit card number, password, etc., without explicit approval from a teacher or administrator;
- pretend to be someone they are not on any digital medium, or otherwise use the network to impersonate another person or entity;

- distribute or access pornography;
- plagiarize, cheat, or otherwise violate the school's academic code of conduct; or
- intentionally infect the school network or any school device with malware (malicious software).

Discipline for Violations

Violation of this policy may be treated as a disciplinary offense under the school's written code of conduct. The code shall set out progressive discipline for such violations, providing for a reprimand or a warning for a first offense, and for subsequent offenses, for school staff to restrict or deny access to the network or other school technologies. Students may be subject to other disciplinary measures when their use of the school network or school technologies violates other provisions of the school's code of conduct, for example rules against profanity, bullying, harassment, cheating, and plagiarism.

Searches of Student Information

Students retain an expectation of privacy in their internet, email, educational apps, computer data, and other digital information. As the Supreme Court has made clear, students do not shed their constitutional rights when they go to school.

Searches Conducted by School Officials

A school official may search an individual student's school email, internet records (including but not limited to search history and educational apps data), or device only when she has a reasonable and individualized—focused on the individual student—suspicion that the search will reveal evidence that the student violated a school district policy pertaining to the conduct of students, as published and made available by the school pursuant to G.L. chapter 71, §37H. Reasonable suspicion must be based on specific and objective facts that the search will produce evidence related to the particular alleged violation. Reasonable suspicion cannot be based on curiosity, rumor, hunch, mere disruptive activity, attempts to hide personal possessions, or invocations of a student's constitutional rights. Searches of an individual student's internet records or computer data may not be conducted in order to search for evidence of another student's or students' violations. Except in emergencies, no school official shall use software or network access to conduct remote searches without the student's and guardian's knowledge.

Prior to conducting any search of a student's digital information, school staff shall: (1) document the individualized facts that constitute the reasonable suspicion justifying the search; (2) notify the student and the student's parent or legal guardian of the particular suspected violation and the type of data to be searched for as evidence of the violation; and (3) provide the student's parent or legal guardian the opportunity to be present during the search. The search must be limited in scope to locating evidence of the suspected policy violation and must be terminated when any such evidence has been located.

Searches Involving Law Enforcement

School officials shall not perform searches of student digital information at the instigation, request, direction, or on behalf of any law enforcement official except (1) when there is an imminent threat to life or safety, as outlined below, or (2) when a law enforcement official presents a probable cause warrant specifying the particular item(s) to be searched and/or seized. Except as provided in the section below, school officials shall not disclose any part of a student's digital information to law enforcement absent a probable cause warrant stipulating the particular information to be searched and/or seized. For the purposes of this policy, School Resource Officers are considered law enforcement, not school officials.

Requiring search warrants for investigations of possible criminal violations protects the integrity of the criminal justice process, the student's rights, and the school district's and staff's interests.

Searches in Cases of Emergency

When there is an immediate threat to life or safety, school staff or law enforcement officials may search a student's digital information without providing advanced notice or obtaining a warrant. Within 72 hours of accessing records or devices in response to an emergency situation, the school employee or law enforcement official who took that action shall provide a written description of (1) the threat, (2) the reasons for accessing the particular device or service, (3) a description of the search, and (4) the data accessed and/or seized to the student whose records or devices were searched, to the student's parents or legal guardians, and to the school principal's office.

Log of Searches

The school principal's office shall maintain a log in which the following information shall be recorded for each search of a student's digital information or device by school staff or other public employees: the name of the school official or other public employee accessing the records or device; the business address and other contact information for the person accessing the records or device; the date of access; the data or functions accessed; and the basis for the search. The log shall include documentation of searches undertaken in emergencies. Logs maintained pursuant to this provision shall not contain any personally identifiable student data, shall be made available to members of the public upon request, and shall be public records subject to the public records law, G.L. chapter 66, §10.