



**P 5133
Students**

USE OF PRIVATE TECHNOLOGY DEVICES BY STUDENTS

Students may possess privately owned technological devices on school property and/or during school-sponsored activities, in accordance with the mandates of this policy and any applicable administrative regulations as may be developed by the Superintendent of Schools.

Definitions

District Technology Resources

For the purposes of this policy, “District technology resources” refers to the Regional School District 10 computers and instructional technologies; communications and data management systems; informational technologies and the Internet; and any other technology resources owned and/or used by the school district and accessible by students.

Privately Owned Technological Devices

For the purposes of this policy, “privately owned technological devices” refers to privately owned desktop computers, wireless and/or portable electronic hand-held equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing, etc. These devices may include, but are not limited to, desktops, laptops, smartphones, network access devices, tablet computers, and other electronic signaling devices.

Use of Privately Owned Technological Devices

Privately owned technological devices may not be used during instructional time, except as specifically permitted by instructional staff or unless necessary for a student to access the district’s digital learning platform or otherwise engage in remote learning.

On school property, at a school-sponsored activity, while in use for a remote learning activity, or while being used to access or utilize District technology resources, the use of any such device for an improper purpose is prohibited. Improper purposes include, but are not limited to:

- Sending any form of a harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime);

- Gaining or seeking to gain unauthorized access to District technology resources;
- Damaging District technology resources;
- Accessing or attempting to access any material that is obscene, obscene as to minors, or contains pornography;
- Cyberbullying;
- Using such device to violate any school rule, including the unauthorized recording (photographic, video, or audio) of another individual without the permission of the individual or a school staff member; or
- Taking any action prohibited by any Federal or State law.

Search of Privately Owned Technological Devices

A student's privately owned technological device may be searched if the device is on school district property or in a student's possession at a school-sponsored activity and if there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school. Any such search shall be reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.

Responsibility for Privately Owned Technological Devices

Students are responsible for the safety and use of their privately owned technological devices. If a privately owned technological device is stolen, lost, or damaged while the device is on school property or during a school-sponsored activity, a report should be made to the building principal, who will investigate the loss in a manner consistent with procedures for stolen or damaged personal property. Students and parents should be aware that the District is not liable for any privately owned technological device that is stolen, lost, or damaged while at school or during a school-sponsored activity. For that reason, students are advised not to share or loan their privately owned technological devices with other students.

Disciplinary Action

Misuse of the District's technology resources and/or the use of privately owned technological devices to access or utilize the District's technology resources in an inappropriate manner or the use of such devices in any manner inconsistent with this policy will not be tolerated and will result in disciplinary action. For students, a violation of this policy may result in loss of access privileges, a prohibition on the use and/or possession of privately owned technological devices on school property or at school-sponsored activities, and/or suspension or expulsion in accordance with the Board's policies related to student discipline.

Access to District Technology Resources

The District may permit students, using their privately owned technological devices, to access the District's computers and instructional technologies; communications and data management systems; informational technologies and the Internet; and any other technology resources used by the school district and accessible by students. Additionally, it is the expectation of the District that students who access these resources while using privately owned technology devices will act at all times appropriately in ways which are fully in accord with applicable policies concerning technology use as well as all local, state, and federal laws.

Through the publication and dissemination of this policy statement and others related to use of the District's computer systems, as well as other instructional means, the District educates students about the District's expectations for technology users.

The District technology resources shall only be used to access educational information and to promote learning activities both at home and at school. Students are expected to act at all times appropriately in ways which are fully in accord with applicable policies concerning technology use as well as all local, state, and federal laws when using the District technology resources. Failure to do so will result in the consequences outlined herein and in other applicable policies (including, but not limited to, the Safe School Climate Plan, the Student Discipline Policy and the Use of Computers Policy).

Students must abide by the procedures outlined in this policy and all policies and applicable regulations outlined in the Board's computer use and other applicable policies. Students will be given specific information for log-on and access procedures for using school accounts. No user may deviate from these log-on/access procedures. **Students are advised that the District's network administrators have the capability to identify users and to monitor all privately owned technological devices while they are logged on to the network.** Students must understand that the District has reserved the right to conduct monitoring of District technology resources and can do so *despite* the assignment to individual users of passwords for system security. Any password systems implemented by the District are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user. The system's security aspects, message delete function and personal passwords can be bypassed for monitoring purposes. Therefore, students should be aware that they should not have any expectation of personal privacy in the use of privately owned technological devices to access District technology resources. This provision applies to any and all uses of the District's technology resources and any privately owned technological devices that access the same.

Harm to District Technology Resources

Any act by a student using a privately owned technological device that harms the District technology resources or otherwise interferes with or compromises the integrity of District technology resources will be considered vandalism and will be subject to discipline and/or appropriate criminal or civil action.

Closed Forum

This policy shall not be construed to establish a public forum or a limited open forum.

Legal References:

Conn. Gen. Statutes

§ 10-233j

§ 31-48d

§§ 53a-182; 53a-183; 53a-250, *et seq.*

Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 28
U.S.C. §§ 2510 through 2520

ADOPTED: November 14, 2022

REVISED: October 17, 2022