

Instruction

Bring Your Own Device

Policy Statement

It is the policy of the Regional School District 12 Board of Education to permit access by students and employees using privately-owned electronic devices to the Region's computers, Region issued personal data devices (including smartphones, Blackberries, PDAs, other mobile or handheld devices) and instructional technologies; communications and data management systems; informational technologies and the Internet; and a variety of other technology resources (collectively the "Region technology resources") in order to promote educational excellence. While the Region intends to permit such broad access, the Region's technology resources have not been established as a public access service or as a public forum. Additionally, it is the expectation of the Board of Education that students and employees who access these resources while using personal electronic devices will act at all times in responsible and ethical ways which are fully in accord with the Region's Responsible and Acceptable Use Policies (6141.321 or 4118.5/4218.5) and with all local, state, and federal laws.

Through the publication and dissemination of this policy statement, as well as other instructional means, the Region educates students and employees about the Region's expectations for technology users outlined in its Responsible Use Policies. The Region will also provide professional development to employees regarding their responsibilities and duties while using personal electronic devices to access Region technology resources. Other members of the school community will be informed as appropriate.

The Region will work together with the parents or guardians of students to educate students about the Region's expectation that all students will act responsibly and ethically when accessing and using Region 12 technology resources, including times when access is achieved through the use of personal technology. With students able to access the Region's technology resources, not only from Region 12 devices, but also from privately-owned electronic devices, it is important for each student to have the opportunity to learn about his/her rights, responsibilities, and duties when using personal electronic devices to access technology resources. Through the dissemination of the Student Handbook, the explanation and signing of the Responsible Use Policy (6141.321) and its regulations and protocols, and through presentations by teachers and/or administrators at the beginning of each school year, the Region will inform students of the applicable expectations regarding access to the Region's technology resources when using personal electronic devices on or near school property, at home, in school vehicles and busses, or at school-sponsored activities.

The Region's technology resources shall be used to access educational information and to promote learning activities both at home and at school. The Region considers access to its technology resources to be a privilege and not a right. Employees and students are expected to make responsible and ethical decisions at all times when using the Region's technology resources. Failure to do so will result in the consequences fully outlined in the Responsible Use Policy for Students (6141.321), in the Acceptable Computer Network Use (4118.5/4218.5), and in other related policies.

Definitions

Region Technology Resources

For the purposes of the Region's BYOD policy, "Regional Technology Resources" refers to Region's computers, Region issued personal data devices (including Smartphones, Blackberries, PDAs, Smartphones,

other mobile or handheld devices) and instructional technologies; communications and data management systems; informational technologies and the Internet; and a variety of other technology resources in order to promote educational excellence.

Employee

For the purposes the Region's BYOD policy, the term "employee" shall be deemed to include contractors, volunteers, Board of Education members, third parties and other non-student members of the school community.

Personal Technology

For the purposes of the Region's BYOD policy, "personal technology" refers to privately owned 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, personal laptops, smartphones, network access devices, and other electronic signaling devices.

Personal Technology Security

Responsibility for keeping personal technology secure rests with the individual owner. If personal technology is stolen, lost, or damaged, it will be handled through the administrative office similar to how other stolen, lost, or damaged personal artifacts are handled. Employees, students, and parents should be aware that the Region is not liable for any personal technology that is stolen, lost, or damaged. Students should not share their personal technology with other students at any time.

Region Technology Resources/Damages

Virtual or physical vandalism shall not be tolerated. Any intentional act by a user of the Region's technology resources that damages, or interferes with the performance of Region hardware, software, operating systems, or communication and data management systems will be considered vandalism and will be subject to discipline and/or appropriate criminal or civil action.

Protocols for Using Personal Technology

Students and employees must abide by all specific protocols outlined in this BYOD policy and all policy and applicable regulations outlined in the Responsible Use Policy for Student Use of Technology Resources (6141.321) and in the Acceptable Computer Network Use (4118.5/ 4218.5). Students and employees will be given specific information for log-on and access procedures using school accounts. No user may deviate from these log-on/access procedures. Students and employees are advised that the Region's network administrators have the capability to identify users and to monitor all BYOD devices while they are logged on to the network.

Users must understand that the Region has reserved the right to conduct monitoring of Regional technology resources and can do so despite the assignment to individual users of passwords for system security. Any password systems implemented by the Region 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, users must be aware that they should not have any expectation of personal privacy in the use of personal technology to access Region technology resources. This provision applies to any and all uses of the Region's technology resources and Region or personal electronic devices that access same.

Disciplinary Action

Misuse of the Region's technology resources and/or the use of personal technology to access or utilize the Region's technology resources in an inappropriate manner will not be tolerated and will result in disciplinary action.

For employees, such misuse may result in disciplinary action up to and including termination of employment. As no two situations are identical, the Board reserves the right to determine the appropriate discipline for any particular set of circumstances.

For students, misuse may result in loss of access privileges, a prohibition on the use and/or possession of personal technology on school property, and/or suspension or expulsion in accordance with the Board's policies related to student discipline.

For other members of the school community, misuse may result in loss of access privileges, a prohibition on the use and/or possession of personal technology on school property, referral to the local police, or other appropriate consequences as befit the specific situation.

(cf. [4118.5/4218.5](#) Acceptable Computer Network Use)

(cf. [6141.321](#) Student Responsible Use Policy for Use of Region Technology Resources)

(cf. [5131.911](#) Bullying Behavior in Schools)

(cf. [5131.913](#) Cyberbullying and the Use of Technology to Harm Others)

(cf. [5145.5](#) Sexual and Other Unlawful Harassment) (Students)

(cf. 4118.112 Sexual and Other Unlawful Harassment) (Staff)

Legal References:

Conn. Gen. Stat. § [31](#)-48d

Conn. Gen. Stat. §§ [53a](#)-182; [53a](#)-183; [53a](#)-250

Electronic Communication Privacy Act, [28](#) U.S.C. §§ 2510 through 2520

Policy adopted: September 24, 2012