

This school district recognizes the importance of providing a positive, productive and engaging learning environment that prepares all students to be career and college ready. Accessing and using technology such as computers and mobile computing devices is a significant component of achieving this goal. This policy, in conjunction with the district's Acceptable Use of Internet, Computer, Mobile Computing Devices, and Network Resources Policy (Policy 942), describes acceptable rules of use by students of district-issued mobile computing devices.

DISTRIBUTION OF MOBILE COMPUTING DEVICES

Prior to issuance of a mobile computing device, each student will be required to sign the district's Acceptable Use of Internet, Computer, Mobile Computing Devices, and Network Resources User Agreement (Policy 942F1). Parents/guardians will also be required to sign the Agreement, regardless of whether the student is over age 18. The Agreement is valid for each school year and must be signed each time a device is issued to a student.

Devices must be returned at the end of each school year, provided that the district may issue devices to support summer school programs. The Superintendent will establish procedures for issuance and return of devices, including maintenance of records to track device inventory and which device is issued to which student.

CARE AND SAFETY

Students are responsible for the general care of the device issued by the district and are expected to observe precautions including, but not limited to:

1. No food or drink is allowed next to a device while it is in use;
2. The device should be shut down when it is not in use to conserve battery life;
3. Devices should not be left in any unsupervised area, such as computer labs, locker rooms, library, hallways, cafeteria, or unlocked classrooms;
4. Students may not place stickers or drawings on the device;
5. Devices should be kept free of anything that could put pressure on the screen;
6. Screens should be cleaned periodically with an anti-static cloth or other soft, dry cloth;
7. Devices should not be stored in areas subject to extreme temperatures;
8. Cables, cords and removable storage devices should be inserted and stored carefully.

The Superintendent will designate an individual or office at the school level where devices must be taken if they break or fail to work properly. Students are expected to report all device problems to the designated individual or office. Students are responsible for any damage to the device caused by negligent acts. Students and parents/guardians will be notified of their responsibility for lost and damaged devices.

Students are expected to password protect their devices and to keep their password confidential.

USE AT SCHOOL

Students are expected to bring their device to class each day, unless specifically advised not to do so by their teacher. Devices should be fully charged each day and power cords must stay with the device at all times. Students who repeatedly fail to bring their device, fail to keep the power cord with the device or fail to bring their device in a fully charged condition will be subject to disciplinary action.

Students who leave their device at home may use a school computer or, if available, a device from a lending pool, at the administrator's discretion. This includes students whose devices are undergoing repair.

During class, sound must be muted or headsets must be used, unless the teacher directs otherwise.

PERSONALIZATION

While the device at all times remains the property of the district, students may place individualized items on the device, such as music, pictures or other items that do not hinder the network or device functionality.

Students may be permitted to select their own screen savers and backgrounds, provided they do not violate district policy against use of guns, weapons, pornographic materials, inappropriate or obscene language, alcohol, drugs, or gang related symbols or pictures. Student passwords or other items deemed inappropriate by administration will result in disciplinary action. Students should also keep in mind that as district property, the district reserves the right to access or view any personal items placed on the device at any time, for any reason, including randomly selected device reviews. Students and parents/guardians have no expectation of privacy in any material placed on the device and any such material is not privileged or confidential.

FILE MANAGEMENT

Students are expected to back up their work using removable file storage, saving to school-provided accounts, or by emailing documents to themselves. Device malfunctions will not be considered an acceptable excuse for failing to submit work in a timely manner.

SOFTWARE

Prior to issuance to students, the district will install software on the device that has been approved for use by the district. This software must remain in working condition and accessible at all times while in the student's possession. The district reserves the right to update, delete or otherwise modify software in accordance with software licenses and district policy. All devices will also be equipped with anti-virus protection software which will be upgraded regularly.

Students are not permitted to upload additional software to the device without first receiving written permission to do so from authorized district staff. Any additional software must be

appropriate for the school environment and comply with Policy 942, Acceptable Use of Internet, Computers, Mobile Computing Devices and Network Resources. Games and device images containing obscene or pornographic material will not be approved and, if found on a student's device will subject the student to disciplinary action.

INSPECTION AND FILTERING

In accordance with Policy 942, filtering software will be used to prevent access to material considered inappropriate or harmful to minors. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 18 and older.

Students may be selected at random or for cause to provide their device for inspection to ensure compliance with district policies regarding student use of technology. The district reserves the right to monitor, inspect, copy, review, delete, and/or store at any time and without prior notice any and all results of usage of the Internet, computers, mobile computing devices, network resources, and any and all information transmitted or received in connection with such usage, including electronic mail, network usage and all stored files on any mobile computing device. All such information will be and remains the property of the district and users have no expectation of privacy regarding such materials. The district has the right to place restrictions on the use of the district's Internet, computers, mobile computing devices, and network resources and may also deny access to staff and students who violate related policies and procedures.

Devices may be equipped with the ability to be accessed remotely. A student does not need to be asked for permission prior to remote access for software maintenance or other inspection.

The district may report violations of this policy to law enforcement and will cooperate fully with all local, state and federal officials in any investigation concerning or relating to violations of law.



LEGAL REFERENCE:

Children's Internet Protection Act (CIPA)(Pub. L. 106-554)(47 U.S.C. §254)

Idaho Code Sections:

6-210 – Recovery of Damages for Economic Loss Willfully Caused by a Minor

18-1514 – Obscene Materials – Definitions

18-2201 – Computer Crime – Definitions

18-2202 – Computer Crime

33-512 – Governance of Schools

CROSS-REFERENCE:

Policy 942 –Acceptable Use of Internet, Computers, Mobile Computing Devices, and Network Resources

Policy 942F1 – Acceptable Use of Internet, Computers, Mobile Computing Devices, and Network Resources for Students User Agreement

ADOPTED: November 20, 2023

AMENDED: