Policy 3275 – District Provided Mobile Computing Devices

~~3275A1~~
~~Alternative 1:~~ Students Allowed to Take Devices Home

The Preston School District #201 is committed to providing a safe, rigorous, and engaging learning environment that prepares all students to be career and college ready. Accessing and using technological resources is one of the cornerstones of a 21st century education. This document describes the rules for acceptable use of District-issued mobile computing devices on and off District premises. Using these resources responsibly will promote educational excellence by facilitating resource sharing, fostering creativity, and promoting communication in a safe, secure environment for all users.

Distributing Mobile Computing Devices

Before they are issued a mobile computing device, each student must submit an executed Student Agreement for Mobile Computing Device Use and a copy of the Internet Access Conduct Agreement. Each form must be signed by the student and by their parent or guardian if they are less than 18 years of age.

The District may provide parent orientations on the mobile computing device program. A student's parents/guardians are encouraged to attend an orientation before the student takes a device home with them.

~~**[OPTIONAL]** Parents or guardians of students may use the school-issued device, and their involvement in student learning through technology is strongly encouraged. However, use of school-issued technology outside of this purpose, such as for personal gain or activities unrelated to student learning, is prohibited. Both parent and student use of the District's device, network, and software may be subject to a public records request depending upon the content of the document or communication, including email.~~

~~Students may take the devices out of Idaho at the discretion of the building principal. The District directs the Superintendent to establish procedures for students to request permission to take the device with them.~~

At the end of the school year, the school will collect all devices from students. At the school's discretion, students may be issued devices to support summer school programs.

The ~~Superintendent~~ school shall establish procedures for the maintenance of records regarding the devices, including tracking device inventory and which device is issued to which student.

Care and Safety

Students are responsible for the general care of the device they have been issued by the District and are expected to observe the following precautions:

1. No food or drink is allowed next to a device while it is in use;
2. Insert and remove cords, cables, and removable storage devices carefully;
3. Shut down the device when not in use to conserve battery life;
4. Stickers, drawings, or permanent markers may not be used on the device;
5. Do not vandalize the devices or any other school property;
6. Devices must never be left in any unsupervised area.
7. Students are responsible for keeping their device's battery charged for school each day;
8. Do not place anything near the device that could put pressure on the screen;
9. Clean the screen with an anti-static cloth or any other soft, dry cloth;
10. Devices should not be stored in a student's vehicle, or anyplace else subject to extreme temperatures;
11. ~~**[INSERT ADDITIONAL PRECAUTIONS SUGGESTED BY MANUFACTURER]**~~

The Superintendent will designate an individual or office at the school level where the devices must be taken if they break or fail to work properly.

~~Use at School~~

~~Devices are intended for use at school each day. Students are responsible for bringing their device to all classes, unless specifically advised not to do so by their teacher. Devices must be brought to school each day in a fully charged condition. Power cords must stay with the device at all times. Repeated failures to comply with these requirements will result in disciplinary action.~~

~~If students leave their device at home, they may phone their parent/guardian to bring it to school. Students without a device will use a computer in the classroom or a device from the lending pool depending upon availability and at the administrator's discretion. This includes students whose devices are undergoing repair.~~

~~Sound must be muted or headsets must be used at all times unless the teacher directs otherwise.~~

~~Students may use printers in classrooms, the library, and computer labs with a teacher's permission during class or breaks. All printing should be limited to educational purposes.~~

Personalizing Mobile Computing Devices

~~**CHOOSE ONE OPTION FROM THE FOLLOWING:**~~

~~**[OPTION 1]** While at no time does the device become the personal property of students or staff; students may place individualized items on the device, which are limited to music, pictures, and 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 are appropriate. Screensavers, backgrounds, or other pictures containing guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, gang related symbols or pictures, the student's password or other items deemed inappropriate by the administration will result in disciplinary actions.~~

~~Students may not add options or upgrades to the device, change the operating system, or add unauthorized software or safety controls.~~

~~Should students or parents/guardians place personalized items on the device, such items may be accessed or viewed by District staff at any time, for any reason, including randomly selected device reviews. No content placed on District provided devices is privileged or confidential~~.

~~**[OPTION 2]**~~ Students may not add options or upgrades to the device, change the operating system, or add unauthorized software or safety controls.

Should students or parents/guardians place personalized items on the device in violation of this policy such items may be accessed or viewed by District staff at any time, for any reason, including randomly selected device reviews. No content placed on District provided devices is privileged or confidential.

Managing Files

Once details are known about the availability of file space that is shared or is backed up automatically, the Superintendent will set a procedure for where students and teachers should save important documents.

Students should also back up their work. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work.

Software

The software originally installed by the District must remain on the device in usable condition and be easily accessible at all times.

From time to time the school may add or update software applications. The licenses for

this software sometimes require that the software be deleted from devices at the completion of a course. Periodic reviews of devices will be made to ensure that students have deleted software that is no longer required in class and that the school has not exceeded its licenses.
All devices will be equipped with anti-virus protection software which will be upgraded regularly.

It is the responsibility of individual students to be aware of additional software programs and files loaded onto their device which are required for classes or school activities. Students wishing to load additional software onto a device must first obtain the permission of the school's technology department. Any additional software must be appropriate for the school environment and comply with the Internet Access Conduct Agreement. Violent games and device images containing obscene or pornographic material are banned. The technology department shall determine whether a game is violent, and the student may appeal this decision to the principal. Each student is responsible for ensuring that only licensed software is loaded onto their device.

Students shall refrain from downloading the TikTok app onto any District issued device. If TikTok has already been downloaded onto a device issued to a student, the student shall delete the app or seek assistance from District technology personnel OR the building principal in deleting it.

Inspection and Filtering

Filtering software will be used to prevent access to material considered inappropriate or harmful to minors.

~~**[OPTIONAL]** 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. If technical difficulties occur or unauthorized software or any other violation of District policy is discovered, all files and the hard drive may be reformatted. Only authorized software will be installed. The District does not accept responsibility for the loss of any software or other materials deleted due to a reformat and reimage.

Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. The District will cooperate fully with local, State, or federal officials in any investigation concerning or relating to violations of law.

Remote Access of Devices

Devices may be equipped with the ability to be accessed remotely in the case of technical problems requiring remote assistance, missing or stolen devices, or other for any other appropriate District purpose. A student does not need to be asked for permission prior to remote software maintenance.

Acceptable Use

Access to the devices is a privilege and not a right. Each employee, student, and parent will be required to follow the Internet Access Conduct Agreement and the Acceptable Use of Electronic Networks Policy. Violation of these policies, whether by the student or another party, while the device is in student custody may result in disciplinary action for the student, possible revocation of device privileges, and/or contacting law enforcement authorities.

Protecting and Storing Devices

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

When students are not using their devices, the devices should be stored in their lockers. Students are encouraged to take their devices home every day after school.

Under no circumstances should devices be left in unsupervised areas. Unsupervised areas include the school grounds, the cafeteria, computer lab, locker rooms, library, unlocked classrooms, dressing rooms, and hallways. Unsupervised devices will be confiscated by staff and taken to the building principal's office. Disciplinary action may be taken for leaving a device in an unsupervised location.

Repair of Devices

Students are to report all device problems to ~~**[District technology personnel OR the building principal].**~~ the teacher.

The Superintendent will issue a document clarifying student or parent responsibility for lost and damaged devices when the details of the District's insurance policy are known.

~~3275A2~~
~~Alternative 2: Students Not Allowed to Take Devices Home~~

~~The {{Full_District_Name}} is committed to providing a safe, rigorous, and engaging learning environment that prepares all students to be career and college ready. Accessing and using technological resources is one of the cornerstones of a 21st century education. This document describes the rules for acceptable use of school-~~

issued mobile computing devices. Using these resources responsibly will promote educational excellence by facilitating resource sharing, fostering creativity, and promoting communication in a safe, secure environment for all users.

Distributing Mobile Computing Devices

Before they are issued a device, each student must submit a Student Mobile Computing Device Agreement and a copy of the Internet Access Conduct Agreement. Each form must be signed by the student and by their parent or guardian if they are less than 18 years of age.

At the end of the school year, the school will collect all devices from students. At the school's discretion, students may be issued devices to support summer programs.

The Superintendent shall establish procedures for the maintenance of records regarding the devices, including tracking device inventory, and which device is issued to which student.

Care and Safety

Students are responsible for the general care of the device they have been issued by the District and are expected to observe the following precautions:

1. No food or drink is allowed next to a device while it is in use;
2. Insert and remove cords, cables, and removable storage devices carefully;
3. Shut down the device when not in use to conserve battery life,
4. Stickers, drawings, or permanent markers may not be used on the device;
5. Do not vandalize the device or any other school property;
6. The device must never be left in any unsupervised area,
7. Do not place anything near the device that could put pressure on the screen;
8. Clean the screen with a soft, dry cloth or anti-static cloth;
9. The device should not be stored anyplace that is subject to extreme temperatures;
10. **[INSERT ADDITIONAL PRECAUTIONS SUGGESTED BY MANUFACTURER]**

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.

Use at School

The devices are intended for use at school each day. Students are responsible for bringing their device to all classes, unless specifically advised not to do so by their teacher. Power cords must stay with the device at all times, and the device must be returned for recharging at the end of each school day. Repeated failures to comply with

these requirements will result in disciplinary action.

Students without a device will use a computer in the classroom or a device from the lending pool depending upon availability and the administrator's discretion. This includes students whose devices are undergoing repair.

Sound must be muted or headsets must be used at all times unless the teacher directs otherwise.

Students may use printers in classrooms, the library, and computer labs with a teacher's permission during class or breaks. All printing should be limited to educational purposes.

CHOOSE ONE OPTION FROM THE FOLLOWING:

[OPTION 1] While at no time does the device become the personal property of students or staff; students may place individualized items on the device, which are limited to music, pictures, and 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 are appropriate. Screensavers, backgrounds, or other pictures containing guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, gang related symbols or pictures, the student's password or other items deemed inappropriate by the administration will result in disciplinary actions.

Student may not add options or upgrades to the device, change the operating system, or add unauthorized software or safety controls.

Students shall refrain from downloading the TikTok app onto any District issued device. If TikTok has already been downloaded onto a device issued to a student, the student shall delete the app or seek assistance from **[District technology personnel OR the building principal]** in deleting it.

Should students or parents/guardians place personalized items on the device, such items may be accessed or viewed by District staff at any time, for any reason, including randomly selected device reviews. No content placed on District provided devices is privileged or confidential.

[OPTION 2] Students may not add options or upgrades to the device, change the operating system, or add unauthorized software or safety controls.

Students shall refrain from downloading the TikTok app onto any District issued device. If TikTok has already been downloaded onto a device issued to a student, the student shall delete the app or seek assistance from **[District technology personnel OR the**

building principal] in deleting it.

Should students or parents/guardians place personalized items on the device in violation of this policy such items may be accessed or viewed by District staff at any time, for any reason, including randomly selected device reviews. No content placed on District provided devices is privileged or confidential.

Managing Files

Once details are known about the availability of file space that is shared or is backed up automatically, the Superintendent will set a procedure for where students and teachers should save important documents.

Students should also back up their work. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work.

Software

The software originally installed by the District must remain on the device in usable condition and be easily accessible at all times.

From time to time the school may add or update software applications. The licenses for such software sometimes require that the software be deleted from devices at the completion of a course. Periodic checks of devices will be made to ensure that students have deleted software that is no longer required in class and that the school has not exceeded its licenses.

All devices will be equipped with anti-virus protection software which will be upgraded regularly

It is the responsibility of individual students to be aware of additional software programs and files loaded onto their device which are required for classes or school activities.

Students wishing to add additional software onto a device must first obtain the permission of the school's technology department. Any additional software must be appropriate for the school environment and comply with the Internet Access Conduct Agreement. Violent games and computer images containing obscene or pornographic material are banned. The technology department shall determine whether a game is violent, and the student may appeal this decision to the building principal. Each student is responsible for ensuring that only licensed software is loaded onto their device.

Inspection and Filtering

~~Filtering software will be used to prevent access to material considered inappropriate or harmful to minors.~~

~~**[OPTIONAL]**~~
~~The 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. If technical difficulties occur or unauthorized software or any other violation of District policy is discovered, all files and the hard drive may be reformatted. Only authorized software will be installed. The school does not accept responsibility for the loss of any software or other materials deleted due to a re-format and re-image.~~

~~Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. The District will cooperate fully with local, State, or federal officials in any investigation concerning or relating to violations of law.~~

~~Remote Access of Devices~~

~~Devices may be equipped with the ability to be accessed remotely in the case of technical problems requiring remote assistance, missing or stolen devices, or other for any other appropriate District purpose. A student does not need to be asked for permission prior to remote software maintenance.~~

~~Acceptable Use~~

~~Access to the devices is a privilege and not a right. Each student and/or parent will be required to follow the Internet Access Conduct Agreement and the Mobile Computing Device Acceptable Use Policy. Violation of these policies, whether by the student or another party, while the device is in student custody may result in disciplinary action for the student, possible revocation of device privileges, and/or contacting law enforcement authorities.~~

~~Protecting and Storing Devices~~

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

~~When students are not using their devices, the devices should be stored in their lockers. Students will return the devices for storage and recharging each day at the end of the school day.~~

~~Under no circumstances should devices be left in unsupervised areas. Unsupervised areas include the school grounds, the cafeteria, computer lab, locker rooms, library, unlocked classrooms, dressing rooms, and hallways. Unsupervised devices will be confiscated by staff and taken to the building principal's office. Disciplinary action may be taken for leaving a device in an unsupervised location.~~

~~Repair of Devices~~

~~Students are to report all device problems to **[District technology personnel OR the principal]**.~~

~~The Superintendent will issue a document clarifying student or parent responsibility for lost and damaged devices when the details of the District's insurance policy are known.~~

Legal Reference:

Legal References	Description
47 USC § 254(h)	Telecommunications Services for Certain Providers
47 USC § 254(l)	Internet Safety Policy Requirement for Schools and Libraries
IC § 18-6726	TikTok Use by State Employees on a State-Issued Device Prohibited
Idaho Executive Order	2022-06
Pub. L. 106-554	Children's Internet Protection Act (CIPA)

Cross References

Code	Description
3260	Bring Your Own Technology Program
3260-F(1)	Bring Your Own Technology Program - Permission Form
3270	District-Provided Access to Electronic Information, Services, and Networks
3270-P(1)	District-Provided Access to Electronic Information, Services, and Networks - Acceptable Use of Electronic Networks
3270-F(1)	District-Provided Access to Electronic Information, Services, and Networks - INTERNET ACCESS CONDUCT AGREEMENT

Adopted:
Revised:
Reviewed: