Highland Joint School District #305 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 Internet Access Conduct and Mobile Computing Device Agreement. Each form must be signed by the student and by their parent or guardian if they are less than eighteen years of age.

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

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/or software may be subject to a public records request depending upon the content of the document or communication, including email.

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 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:

- No food or drink is allowed next to a device while it is in use;
- Insert and remove cords, cables and removable storage devices carefully;
- Shut down the device when not in use to conserve battery life.
- Stickers, drawings, or permanent markers may not be used on the device;
- Do not vandalize the devices or any other school property;
- Devices must never be left in any unsupervised area.
- Students are responsible for keeping their device's battery charged for school each day;
- Do not place anything near the device that could put pressure on the screen;
- Clean the screen with a soft, dry cloth or anti-static cloth;

- Devices should not be stored in a student's vehicle, or anyplace else subject to extreme temperatures;

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. Repeat failures to comply with these requirements will result in disciplinary action.

If students leave their device at home, they may phone parents/guardians to bring them to school. Students without a device will use a computer in the classroom or a device from the lending pool depending upon availability 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 teachers' permission during class or breaks. All printing should be limited to educational purposes.

Personalizing Mobile Computing Devices

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 frequently using removable file storage or by e-mailing important document to themselves. 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 and/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 and Mobile Computing Device 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 his/her device.

Inspection and Filtering

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. 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/or parent will be required to follow the Internet Access Conduct and Mobile Computing Device 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.

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.

Cross Reference: 429.1 Internet Access Conduct and Mobile Computing Device Agreement
429.0 Acceptable Use of Electronic Networks

Legal Reference: Technology Task Force Final Task Force Recommendations
Children's Internet Protection Act, P.L. 106-55420 U.S.C. § 6801, et seq.
47 U.S.C. § 254(h) and (l)

• • • • • • •

ADOPTED: 12/10/2012
AMENDED: