Electronic Resources & Internet Safety and One to One Technology Use Rules

Electronic Resources & Internet Safety

The Highland Board of Directors recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The board also believes that staff and students need to be proficient and safe users of information, media, and technology to succeed in a digital world.

Electronic Resources

The district will develop and use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways and for staff to educate them in such areas of need. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings use these tools. The district's technology will enable educators and students to communicate, learn, share, collaborate and create; to think and solve problems; to manage their work; and to take ownership of their lives.

The superintendent or designee will: 1) create strong electronic resources and develop related educational systems that support innovative teaching and learning; 2) provide appropriate staff development opportunities regarding this policy; and 3) develop procedures to support this policy. The superintendent or designee is authorized to develop procedures and acceptable use guidelines for staff and students as to use of district electronic resources, including those that access Internet and social media, and to regulate use of personal electronic resources on district property and related to district activities.

Internet Safety

To help ensure student safety and citizenship with electronic resources, all students will be educated about Internet safety. This will include appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

To promote Internet safety and appropriate online behavior of students and staff as they use electronic resources and access material from the Internet, the superintendent or designee is authorized to develop or adopt Internet safety procedures, acceptable use guidelines, and, for students, related instructional materials for every grade level. The superintendent or designee in evaluating such procedures and instructional materials should take into account District electronic resources, community norms, privacy rights, responsible use, and issues of concern with student or staff use of electronic resources.

As a component of district Internet safety measures, all district-owned electronic resources, including computer networks and Wi-Fi, in all district facilities capable of accessing the Internet must use filtering software to prevent access to obscene, racist, hateful or violent material. However, given the ever-changing nature of the Internet, the district cannot guarantee that a student will never be able to access objectionable material.

Further, when students use the Internet from school facilities for educational purposes, district staff will make a reasonable effort to supervise student access and use of the internet. If material is accessed that violates district policies, procedures or student guidelines for electronic resources or acceptable use, district staff may instruct the person to cease using that material and/or implement sanctions consistent with district policies, procedures, guidelines, or student codes of conduct.

One to One Technology Use Rules

Purpose: Highland School District will provide and assign students a laptop for use both at school and at home to support learning. This policy provides guidelines and expectations for students and families who are issued district laptops. Additional rules may be added and would become a part of this policy.

HSD will maintain and periodically update laptops. Students will be notified of maintenance in advance.

Our expectation and belief is that students will responsibly use district technology and that they understand the appropriate and acceptable use of both the technology, and district networks. We also expect that students will keep their district-issued devices safe, secure and in good working order.

Responsibilities: The student will:

1. Adhere to these guidelines each time the device is used at home and school.
2. Charge their laptop at home nightly and bring it to school each day with a full charge (classrooms will have limited capacity to charge devices during the day).
3. Use appropriate language in all communications avoiding profanity, obscenity and offensive or inflammatory speech. Cyber bullying is to be reported to school personnel immediately. Communication should be conducted in a responsible, ethical and polite manner.
4. Respect the Internet filtering and security measures included on the laptop. All student laptops are configured so that Internet content is filtered both when the student is at school and when on any other public or private network.
5. Use technology only for school-related purposes during the instructional day.
6. Follow copyright laws and fair use guidelines. Students should only download music, video or other content which is related to classroom assignments and which students are authorized or legally permitted to use.
7. Understand that district technology, student files, and student activity may be viewed, monitored or archived by the district at any time. You must make your laptop available for inspection if requested by any administrator, teacher or your parent/guardian.

Restrictions: The student will not:

1. Mark, deface, or place stickers on the laptops, except in the area designated by the district.
2. Reveal or post identifying personal information, pictures, files or communications to unknown persons through email or the Internet.
3. Attempt to override, bypass or otherwise change the Internet filtering software, device settings, or network configurations.
4. Attempt access to networks and other technologies beyond their authorized access. This includes attempts to use another person's account and/or password or access secured wireless networks.
5. Share passwords or attempt to discover passwords. Sharing a password is not permitted and could make you subject to disciplinary action and liable for the actions of others if problems arise with unauthorized use.
6. Download and/or install any programs, files, or games from the Internet or other sources onto any district-owned technology. This includes the intentional introduction of computer viruses and other malicious software.
7. Tamper with computer hardware or software, attempt unauthorized entry into computers, and/or vandalize or destroy the computer or computer files. Intentional or negligent damage to computers or software may result in criminal charges.
8. Use the device to attempt to locate, view, share, or store any materials that are unacceptable in a school setting. This includes but is not limited to pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials. The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school library/media center.

In addition to the specific requirements and restrictions detailed above, it is expected that students and families will apply common sense to the care and maintenance of the district provided laptop. In order to keep laptops secure and damage-free, please follow these additional guidelines:

- Do not loan your laptop or charger and cords to anyone else.
- Do not leave the laptop in a vehicle or leave it unattended at any time.
- Do not eat or drink while using the laptop or have food or drinks in close proximity.
- Keep your laptop away from locations like table edges, floors, seats or pets.
- Do not stack objects on top of your laptop, leave it outside, or use near water.

Just like textbooks, team uniforms and other school property issued to your child for school purposes, there is a responsibility to care for and appropriately use the resource. We know accidents and/or loss may happen, even when students attempt to take good care of the device. In these instances, district policies and state regulations require a fine be levied to cover the repair or replacement cost of district property.

- If a laptop is reported stolen or lost by a student, the parent or guardian must file a police report and bring a copy to school. If it stolen on campus, the student should report it directly to a school administrator.
- If a family leaves the District, but does not return the laptop, they will be fined for the full replacement costs, and standard rules for the restriction of records and transcripts would apply. Law enforcement may be involved for the purpose of recovering district property.
- Willful abuse and/or intentional damage to the laptop (i.e. damage caused by writing on the machine, willful destruction, prying off keys, spilling liquid in the machine, etc.) will be treated as vandalism by the school and may include additional disciplinary action. This includes missing keys from the keyboard (Keys do not just fall off of a laptop keyboard.)

HSD is not responsible for any loss resulting from use of district-issued technology and makes no guarantees that the technology or the district network systems that support student use will be available at all times. By signing this policy you agree to abide by the conditions listed above and assume responsibility for the care and proper use of HSD district-issued technology. You understand that should you fail to honor all the terms of this Policy, access to laptops, the Internet, and other electronic media may be denied in the future. Furthermore, students may be subject to disciplinary action as outlined in the HSD Student Code of Conduct.

Cross References: 2020 - Course Design, Selection and Adoption of Instructional Materials
2023 – Digital Citizenship and Media Literacy
2025 - Copyright Compliance
3207 - Prohibition of Harassment, Intimidation and Bullying
3231 - Student Records
3241 - Classroom Management, Discipline and Corrective Action
4040 - Public Access to District Records
4400 - Election Activities
5281 - Disciplinary Action and Discharge

Legal References: 18 USC 2510-2522 Electronic Communication Privacy Act

Management Resources: 2015 - June Policy Issue
2012 - October Issue
2012 - February Issue

Policy News, June 2008 Electronic Resources
Policy News, June 2001 Congress Requires Internet Blocking at School
Policy News, August 1998 Permission required to review e-mail

Adoption Date: **9/21/10**
Classification: **Priority**
Revised Dates: **6.20.17; 5.15.18;**