

Perkins Local School District Technology Acceptable Use Policy (AUP) Students

Section 1. Purpose of Technology Use

The Perkins Local School District provides technology resources to its students solely for educational purposes. Through technology, the District provides access for students and staff to resources from around the world. Expanding technologies take students and staff beyond the confines of the classroom, and provide tremendous opportunities for enhancing, extending, and rethinking the learning process. The goal in providing these resources is to promote educational excellence in the District by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff.

Section 2. The Opportunities and Risks of Technology Use

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting, or that may be harmful or disruptive. Because information on networks is transitory and diverse, the District cannot completely predict or control what users may or may not locate. The Board of Education believes that the educational value of limited access to the information, interaction, and research capabilities that technology offers outweighs the possibility that users may obtain or encounter material that is not consistent with the educational goals of the District.

In accordance with the Children's Internet Protection Act (Title XVII), the District installs and operates filtering software to limit users' Internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, or disruptive to the educational process, notwithstanding that such software may in certain cases block access to other materials as well. At the same time, the District cannot guarantee that filtering software will in all instances successfully block access to materials deemed harmful, indecent, offensive, pornographic, or otherwise inappropriate. The use of filtering software does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials.

No technology is guaranteed to be error-free or totally dependable, nor is it safe when used irresponsibly. Among other matters, the District is not liable or responsible for:

- Any information that may be lost, damaged, or unavailable due to technical, or other, difficulties;
- The accuracy or suitability of any information that is retrieved through technology;
- Breaches of confidentiality;
- Defamatory material; or
- The consequences that may come from failure to follow district policy and procedures governing the use of technology.

Section 3. Privileges and Responsibilities

The District's electronic network is part of the curriculum and is not a public forum for general use. Student users may access technology for only educational purposes. The actions of student users accessing networks through the District reflect on the District; therefore, student users must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying administrative regulations and guidelines. Students are responsible for their behavior and communications using the District's computers and networks.

Student users of technology shall:

- Use or access District technology only for educational purposes;
- Comply with copyright laws and software licensing agreements;
- Understand that email and network files are not private. Network administrators may review files and communications to maintain system integrity and monitor responsible student use;
- Respect the privacy rights of others;
- Be responsible at all times for the proper use of technology, including proper use of access privileges, complying with all required system security identification codes, and not sharing any codes or passwords;
- Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses;
- Abide by the policies and procedures of networks and systems linked by technology.

Students may not use District technology including property issued under the 1:1 program for improper uses.

These uses include, but are not limited to:

- Any and all illegal purposes;
- Any and all obscene or pornographic purposes, including, but not limited to, sending, retrieving, or viewing sexually explicit material;
- Any and all discriminatory purposes, including harassment and bullying of individuals based on race, gender, religion, sexual orientation, or disability, among others;
- Any and all purposes that would violate state, federal or international law, including The Ohio Student Privacy Law (Ohio Revised Code § 3319.321) and federal law, Family Educational Rights and Privacy Act (FERPA), which govern students' rights to privacy and the confidential maintenance of certain information including, but not limited to:
 - a student's grades and test scores;
 - Copyright laws;
 - Cyberbullying laws;
 - and Sexting laws.
- Any use of profanity, obscenity, or language that is offensive or threatening;
- Re-posting or forwarding personal communications without the author's prior consent;
- Re-posting or forwarding of junk mail, chain letters, or inappropriate or offensive jokes;
- Destruction, alteration, disfigurement or unauthorized access of hardware, software, or firmware;
- Obtaining financial gain or transacting any business or commercial activities;
- Political advocacy;
- Disrupting the use of others to any process, program or tool, including downloading or otherwise spreading computer viruses;
- Engaging in hacking of any kind, including, but not limited to, illegal or unauthorized access;
- Using unauthorized proxy servers and/or virtual private networks (VPN's);
- Allowing others to use property issued under the program without authorization, including staff whose access privileges have been suspended and/or revoked;
- Soliciting or distributing information with the intent to incite violence, cause personal harm, damage a person's character, or to harass another individual.

Section 4. Internet Safety:

Students must take steps to ensure their safety on the internet, including, but not limited to, the following rules:

- Students should never give out identifying information such as home address, school name, or telephone number to others on the Internet or by email, including in a public message such as chat room or newsgroups. If a person asks for such personal information, students must have approval of their parent or guardian before providing the information.
- Students should not post photographs of themselves in newsgroups or on websites that are available to the public. Students should not arrange a face-to-face meeting with someone they "meet" on the Internet or by email without parental/guardian permission. If a meeting is arranged, the meeting must be in a public place and the student's parent/guardian must attend.
- Student Users should not respond to messages that are suggestive, obscene, belligerent, threatening, or make a student user feel uncomfortable. If a student receives such a message, he or she should provide a copy of the message to his or her parent or guardian immediately. If the message requires school action (e.g., bullying) the student's parent should provide a copy to the principal.

The District recommends that parents/guardians read and follow the U.S. Department of Justice Guidelines for Parents/Guardians on Internet Safety located at:

<https://www.justice.gov/criminal-ceos/children-internet-safety>

Section 5. Disciplinary Actions

Violations of this policy, or any administrative regulations and guidelines governing the use of technology, will result in disciplinary action which could include loss of network access, loss of technology use, suspension or expulsion, or other appropriate disciplinary action. Violations of local, state or federal law may subject students to prosecution by appropriate law enforcement authorities.

Section 6. No Expectation of Privacy

The District's electronic network is part of the curriculum and is not a public forum for general use. Users should not expect that email or files stored on District servers, local or remote, will be private. The District reserves the right to log technology use, to monitor file server space utilization by users, and to examine users' files and materials as needed, and at its discretion.

Users must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside the District.

Section 7. Program Agreement / Terms

The District is pleased to offer our students access to the District's computers, network, internet, and other technology, including related hardware and software devices issued through a 1:1 program, (the "District's Technology") for educational purposes. The District Technology is issued to students for their own personal, school-related uses at school and at home. All District Technology issued under the 1:1 program, including computers, are educational tools and may only be used in that capacity. Any use of the District Technology for other purposes (such as personal purposes) must be minimal (*de minimus*) only, and failure to comply may lead to termination of rights under the 1:1 program.

Title/Ownership:

District maintains the legal title of any District Technology issued to students. Students are authorized to possess and use the District Technology so long as they comply with the AUP, but they do not have any ownership rights in the District Technology.

No Warranties:

The District makes no warranties regarding the District Technology. The District shall not be liable for any damage or loss or other claims of any and all kinds resulting directly or indirectly from use or inability to use District Technology.

Section 8. Equipment Care / Extended Warranty

Successful technology use is dependent upon reliable hardware, software, and infrastructure systems. To that end, students are responsible for the care of the computer equipment assigned to them. Every effort should be made to treat each piece of equipment as the delicate instrument it is. For its part, the District provides on-site maintenance and repair computer technicians available to take care of minor equipment problems. Major repair issues are done by a third party vendor who specializes in the repair of the equipment the district uses.

To cover the cost of these larger repairs, and to minimize the impact of these costs to both the district and students, Perkins Local School District has purchased a damage and repair extended warranty. The cost of this additional warranty is charged to students at \$50.00. This will cover the cost of accidental breakage and repairs but will not cover the costs of repairs deemed to be the result of intentional and/or malicious misuse. **The determination of whether damage to a machine is intentional and/or malicious will be done by the third party repair company and the associated repair costs if the machine is deemed to be damaged intentionally will be set by them, up to, and including the cost of full machine replacement.** Failure by the student to pay the repair cost of the machine will result in the loss of machine usage.

This \$50.00 cost covers the planned district life-span of the machine. At the end of the four-year period, students may purchase their laptop for \$1.00.

Lost equipment must be reported to district technology personnel in writing within 24 hours. Stolen equipment must be reported to the police department and district technology personnel within 24 hours. An official police report must be filed at that time. Students are responsible for the cost to replace lost equipment. Students are not responsible for the cost to replace stolen equipment.

**Perkins Local School District
Technology Acceptable Use Policy Agreement (AUP)
Students**

By signing below you are attesting that you have read and understood the contents of the Acceptable Use Policy. This paper must be signed by a Parent or Guardian before the laptop is assigned to the student.

Student Name (Print) _____ Grade _____

Parent/Guardian Signature _____ Date _____

Student Signature _____ Date _____



PLEASE SIGN, TEAR OUT, AND RETURN TO THE ROOM'S SUPERVISOR BEFORE YOU LEAVE.