Horizon Science Academy Elementary
Digital Use Policy

The Internet and digital resources have become a vital part of our information infrastructure. Through technology, the School 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 reshaping the learning process. The goal in providing these resources is to promote educational excellence by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. The School strongly believes in the educational value of the Internet and digital resources and recognizes the potential of such to support our curriculum and student learning in our school.

The Opportunities and Risks of Technology Use:
The School recognizes the potential for misuse, or abuse, which is inherent in the Internet and will make reasonable efforts to protect its students and teachers. With access to information 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 School cannot completely predict or control what users may or may not locate. The School believes that the educational value of filtered 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 school. In accordance with the Children's Internet Protection Act (CIPA), the School operates monitoring and filtering software designed to limit users' Internet access to materials that are harmful, inappropriate, or disruptive to the educational process, notwithstanding that such software may in certain cases block access to other materials as well.

Such filtering software, however, may not adequately protect users from accessing all harmful matter on the Internet. The installation of such software does not relieve harmful matter. 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.

Indemnity:

No technology is guaranteed to be error-free or totally dependable, nor is it safe when used irresponsibly. Among other matters, the School 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 or digital resources;
- Breaches of confidentiality;
- Defamatory material; or
- The consequences that may come from failure to follow School policies and procedures governing the use of technology and digital resources.

Privileges and Responsibilities:

The School's network and digital resources are part of the curriculum and are not a public forum for general use. Student users may access technology and digital resources only in support of education and research, and within the education goals and objectives of the School. The actions of student users accessing digital resources through the school reflect on the school; 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 School's devices, network, resources, and accounts.

Student users of technology and digital resources shall:

- While on campus, or while using school-owned devices, network, resources, and accounts, use or access technology only for educational purposes.
- Comply with copyright laws and software licensing agreements.
- Understand that email and network files are not private. The School may review files and data 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 shall not use technology for improper uses. Prohibited uses include, but are not limited to:

- Any and all purposes that would violate state, federal or international law, including, but not limited to:
    - Laws governing 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.
- While using any other organization’s network or computing resources, violating that organization’s rules for use of its network or computing resources.
- Knowingly bypassing or penetrating any Internet security measures, including gaining entry or “hacking” into systems, disabling protections, or accessing restricted material without authorization.
- Use which assists, supports, or promotes another person’s Internet use in violation of these rules.
- Production, transmission or storage of any communication or material which may be considered:
    - Defamatory, abusive, harassing or threatening toward another person.
    - Communications or materials which denigrate persons based upon race, ethnicity, religion, gender, or disability are prohibited.
    - Promoting, encouraging or supporting the use of controlled substances.
    - Commercial activities by individuals or for-profit entities.
    - Violating another person’s right to privacy.

        - Using a false identity on the Internet.
        - Otherwise prohibited on a school campus or in a workplace.
- Accessing any pornographic, obscene, vulgar or sexually explicit material, or any material which promotes, encourages or supports any unlawful activity.
- Any use which disrupts the educational process, or disrupts others' appropriate use of digital resources.
- Plagiarizing information.
- Reposting or forwarding personal communications without the author's prior consent.
- Vandalism. Vandalism is defined as any malicious attempt to harm, or destroy, anyone else's data, or any attempt to deprive other users of network services or computers. This includes, but is not limited to, the creation and uploading -downloading of viruses or Trojan horse programs, unauthorized tampering with the Control Panel settings for computers, or physical damage to any machine. Vandalism may result in the loss of computer access, disciplinary action, and legal referral.
- Security breach. Security on any network is a high priority because of the many people relying on that network. If you suspect a security problem, notify the appropriate school personnel at once. Never demonstrate the problem to other users. Never use another individual's password or account. Never give your passwords to another person. Any use identified as a security risk will be denied access to the network and may face disciplinary action.
- Any other use which violates School policy.

Digital Citizenship

Students must take steps to ensure safe and positive use of digital resources, including, but not limited to, the following rules:

- Be Polite. Never send, or encourage others to send, abusive messages.
- Use Appropriate Language. Remember that you are a representative of the School, on a non-private system. You may be alone with your computer, but what you say and do can be viewed globally!

- Keep personal information private. Do not give out identifying information such as home address, school name, or telephone number to others on the online or by email, including in a public message such as chat windows or newsgroups. If a person asks for such personal information, students must have approval of their parent or guardian before providing the information.
- Share responsibly. Do not post photographs of yourself or others on social media or on websites that are available to the public without permission from a parent, or guardian.
- Be an upstander. Do not respond to messages that are suggestive, obscene, belligerent, threatening, or make a student feel uncomfortable. If a student sees 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 School administration.
- Do not arrange a face-to-face meeting with someone students "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.
- The School recommends that families read and follow the U.S Department of Justice Guidelines for Parents/Guardians on Internet Safety located at: https://www.justice.gov/usao-ks/internet-safety

No Expectation of Privacy:

The School's devices, network, resources, and accounts are part of the curriculum and are not for general use. Users should not expect that any data stored on school resources will be private. The school reserves the right to log technology use, to monitor 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 school.

Disciplinary Actions:

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