



Technology Acceptable Use Policy

Section 1. Purpose of Technology Use

Lincoln Preparatory School provides technology resources to its students solely for educational purposes. 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 rethinking the learning process. The goal in providing these resources is to promote educational excellence in the school 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 school cannot completely predict or control what users may or may not locate. Lincoln Preparatory School 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 school.

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;
- Breaches of confidentiality;
- Defamatory material; or
- The consequences that may come from failure to follow school policy and procedures governing the use of technology.

Section 3. Privileges and Responsibilities

The school'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 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 computers and networks.

Student users of technology shall

- Use or access school 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 school 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, 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..
 - Copyright laws;
 - Cyberbullying laws; and
 - Sexting laws.
- Any use of profanity, obscenity, or language that is offensive or threatening;
- Reposting or forwarding personal communications without the author's prior consent;
- Reposting 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;
- Plagiarizing (claiming another person's writings as your own);
- 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, the illegal or unauthorized access;
- Allowing others to use Property issued under the program without authorization, including students whose access privileges have been suspended 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.

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 school's administration.

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 4. Disciplinary Actions

Violations of this policy, or any administrative regulations and guidelines governing the use of technology, may 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 5. No Expectation of Privacy

The school'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 school servers will be private. The school reserves the right to log technology use, to monitor fileserver 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 school.

Section 6. Acceptable Use for Students and Staff

- The school is not responsible for school technology, including computers, assigned to a student at any time, including when they are left unsupervised in a classroom, hallway, locker or elsewhere on school technology.
- The student is the only authorized user of his/her assigned computer or other technology. Students may not share or trade their computers or other technology with other individuals, including other students, other than their parents, guardians or school officials.
- Computers and other technology must be used on flat, stable surfaces only.
- Computers and other technology must not be cleaned with cleaners such as Windex.
- Computers and technology must not be marked with markers, stickers or other similar materials unless it has been done by the school administration.
- School applied labels, asset tags and other identifiers may not be removed from computers or other technology.
- Food and drink should not be used near computers or other technology.
- Computers and other technology should not be left in automobiles, as they cannot tolerate extreme heat or cold and may become damaged.
- Students using the school's computer lab MUST be supervised at all times.