LEXINGTON
PUBLIC SCHOOLS

**Laptop/Computer/iPad/Email/Internet**
# Acceptable Use Policy
**2024-2025**

An Acceptable Use Policy (AUP) is a written agreement that outlines the terms and conditions for using district owned technology as well as any personal technology that is on school property.

Lexington Public Schools has adopted the philosophy of 21st Century Learning in order to provide anywhere/anytime educational opportunities to promote higher level thinking skills and ensure academic success for all students. Students in preschool through twelfth grade are exposed to age appropriate technology in the classroom. Students in grades kindergarten through twelve are assigned an iPad to utilize throughout the school day and take home (with parental permission) in order to complete all coursework. The Lexington Public Schools' network facilities are to be used in a responsible, efficient, ethical, and legal manner in accordance with the educational mission of the district.

## Internet Safety

Internet access is coordinated through a complex association of government, regional and state networks. The reliability of this network is dependent upon proper conduct of the end users. It is essential that all users adhere to the Lexington Public Schools' Internet Safety Policy.

These guidelines are provided to promote awareness and responsibilities of each user utilizing the Internet and district owned technology equipment. Students or staff knowingly violating the terms of this policy will be dealt with according to the student or staff discipline policies of the individual school building and Lexington Public Schools and/or civil authorities, and such activities may result in termination of their account/accessibility and/or expulsion from school or termination of employment.

The use of Lexington Public Schools' equipment, digital devices, network resources, and the Internet is a privilege, not a right, and inappropriate use will result in temporary or permanent suspension of those privileges.

## General Rules & Expectations

The use of district account and/or access must be consistent with the educational objectives of the Lexington Public Schools. Use of electronic resources for recreational games is prohibited.

To transmit or knowingly receive any materials in violation of any United States, Nebraska, or Lexington Public Schools' regulation or law is prohibited. Such materials include but are not limited to the following:

- Pornography
- Obscene, Profane, or Hate Related Material
- Materials related to the illegal use or manufacture of restricted substances
- Defamatory or Discriminatory Material
- Copyrighted Material

Commercial activities, product advertising, and political lobbying are prohibited.

**Network Etiquette –** Users of Lexington Public Schools' Technology and Internet Resources are expected to adhere to the following rules:

- Be polite. Do not be abusive in your messages to others.
- Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language, material, or images.
- Do not reveal your full name, phone number, home address, or personal information of any other person.
- E-mail and other digital use or storage is not guaranteed to be private or confidential. Network or other digital uses or storage areas are and will be treated as school property. It is the right of LPS administration to access and review digital files and communications at any given time.
- It is strictly prohibited to use a digital device or district network resources in a manner that disrupts others, is harmful to others, or invades another person's privacy.

**Safety & Security of Minors**

Internet filtering blocks users from accessing sites that may contain material deemed inappropriate. The federal government has Internet filtering laws that apply to public schools and libraries. These laws stem from the Children's Internet Protection Act (CIPA) which grants federal funds to public schools that abide by the outlined regulations. Such regulations require the School Board to adopt an Internet Use Policy that limits and/or bans minors from gaining access to inappropriate materials such as explicit sexual content or other harmful sites.

Categories that are blocked by Lexington Public Schools' Filter include:

- Adult Content
- Pornography/ Child Pornography
- Nudity
- Illegal File Sharing

- Streaming Radio & TV
- Web Proxies & VPN's (Virtual Private Networks)

In conjunction with its filtering solution, Lexington Public Schools has implemented a report system that monitors school-issued devices web traffic when students are on school grounds and when the device is taken off site.

**E-mail**

All school email addresses and correspondence relating to the use of school email, are the property of Lexington Public Schools. The following rules apply to any/all district email:

- Messages should be professional and courteous.
- Messages must not contain any illegal, libelous, or offensive statements.
- All statements meant to harass — sexually or otherwise — are strictly prohibited.
- Correspondence is for educational purposes only.
- LPS has the right to access e-mail sent to/from every district device.
- LPS has the right to retrieve email stored on its servers that users have deleted from their email.

Students or staff who violate the e-mail policy will be subject to disciplinary measures.

**Chat Rooms/ Social Networking Sites**

Access to all chat rooms and social networking sites shall be strictly prohibited without prior written consent from district administration.

**Consequences/Violations**

Students who fail to abide by district network and Internet access procedures shall be subject to disciplinary action, possible revocation of the user account, and legal action as appropriate. Potential consequences may include, but not be limited to:

- Restricted access to the network and Internet
- Loss of access to the network and Internet
- Possible suspension or expulsion
- Referral to law enforcement

**Bullying/Cyberbullying**

Cyberbullying is using the Internet or other mobile devices to send or post harmful or cruel text or images to bully others. Cyberbullying can take the form of a message on e-mail or instant message or a social networking site from someone who is threatening to hurt you.

The following is a list of common types of cyberbullying:

- Harassment –sending nasty, mean, or insulting messages.
- Flaming- online fights using electronic messages with angry and vulgar language.
- Denigration- sending or posting gossip or rumors about a person to damage his/her reputation.
- Impersonation- pretending to be someone else and sending or posting material to get that person in trouble or danger.
- Outing- sharing someone's secrets or embarrassing information or images online.
- Trickery- tricking someone into revealing secrets or embarrassing information and sharing it online.

If you feel you have been bullied, harassed or threatened online, contact your school's counselor, social worker or principal.

**Hacking/Unauthorized Access**

Hacking, the use of proxies, or bypassing school security systems without prior consent is strictly prohibited.

**Vandalism**

Vandalism will result in the restriction or cancellation of user privileges. Vandalism includes the intentional uploading, downloading, or creating computer viruses, and/or any malicious attempt to harm or destroy district equipment or materials or the data of any other user.

**Children's Internet Protection Act (CIPA)**

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library digital devices. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

The protection measures must block or filter Internet access to pictures that are:

- Obscene
- Pornography
- Child Pornography
- Harmful to Minors

Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet
- Safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications
- Unauthorized access including so-called “hacking” and other unlawful activities by minors online
- Unauthorized disclosure use and dissemination of personal information regarding minors
- Measures restricting minors’ access to materials harmful to them

**Copyright Compliance Policy**

Copyright is defined as a form of protection provided by the government of the United States to the authors of "original works of authorship, including literary, dramatic, musical, artistic, and certain other intellectual works." Copyright is available to both published and unpublished works, regardless of the nationality or domicile of the author. It is unlawful for anyone to violate any of the rights provided by copyright law to the owner of the copyright. Works of authorship include the following categories:

- Literary works
- Musical works, including any accompanying words
- Dramatic works, including any accompanying music
- Pantomimes and choreographic works
- Pictorial, graphic, and sculptural works
- Motion pictures and other audiovisual works
- Sound recordings
- Architectural works

**Resources/Links**

**US Department of Education**

http://www.ed.gov/

**Nebraska Department of Education**

http://www.education.ne.gov/

**Children's Internet Protection Act**:

http://www.fcc.gov/guides/childrens-internet-protection-act

**Protecting Children in the 21st Century Act**

https://www.ftc.gov/legal-library/browse/statutes/protecting-children-21st-century-act

**Stop Bullying Act**

http://www.stopbullying.gov/

**Network Etiquette (Netiquette)**

http://www.networketiquette.net/

**A Parent's Guide to Internet Safety**

https://www2.fbi.gov/publications/pguide/pguidee.htm

**Copyright Compliance**

https://www.copyright.com/learn/media-download/copyright/