Board Adopted: November 08, 2023
Revised and Board Approved: November 08, 2023

2.014 ACCEPTABLE USE OF THE INTERNET

I. Internet Acceptable Use Policy

Riverside Leadership Academy provides students with Internet access to support education and research. Access to the Internet is a privilege subject to restrictions set by the Board of Directors. Violation of any provisions in the Acceptable Use Policy (AUP) may result in disciplinary action and/or cancellation of student access to the Riverside Leadership Academy network. This policy applies to all Internet access on Riverside Leadership Academy property, including Internet access using mobile devices.

II. Access to Information

The Internet gives students access to sites all over the world. Riverside Leadership Academy cannot completely control the information available to students. However, The Children's Internet Protection Act (CIPA) is a federal law enacted to address concerns about access to the Internet and other information. Under CIPA, schools must certify that they have certain Internet safety measures in place.

These include measures to block or filter pictures that;

(a) are obscene,
(b) contain child pornography, or
(c) when computers with Internet access are used by minors, are harmful to minors.

Riverside Leadership Academy monitors online activities of minors to address;

(a) access by minors to inappropriate matter on the Internet and World Wide Web,
(b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications,
(c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online,
(d) unauthorized disclosure, use, and dissemination of personal information regarding minors, and
(e) restricting minors' access to harmful materials.

Riverside Leadership Academy certifies that it is in compliance with CIPA.

Riverside Leadership Academy will monitor the online activities of students and use content filtering software to provide Internet monitoring and content filtering for all students, staff, and visitors on the Riverside Leadership Academy network. The filtering software is intended to allow valuable Internet content, while prohibiting access to obscene material, including pornographic and other content that is harmful to minors. Although it may be possible for a student to find inappropriate material, Riverside

Leadership Academy feels the educational benefit provided by the Internet outweighs any possible disadvantages. Students are prohibited from using or accessing Internet sites containing pornographic, violent or other unacceptable content either at school or at home using school-owned computers/technology/electronic devices. Accessing, producing, posting, displaying or sending offensive messages, music or images, including images of exposed body parts is prohibited. Offensive material includes but is not limited to obscene, profane, lewd, vulgar, rude or sexually suggestive language or images. We encourage parents/guardians to talk with their students about sites and material which the parents believe are inappropriate. Riverside Leadership Academy cannot accept responsibility for enforcing specific parental restrictions that go beyond those imposed by the school. Furthermore, students who bring their own devices to campus are encouraged to take reasonable precautions to ensure the security of those devices. This includes operating system updates and virus scanning.

Students who bring their own devices to campus are encouraged to take reasonable precautions to ensure the security of those devices. This includes operating system updates and virus scanning.

III. Acceptable Uses

All Internet use by students at Riverside Leadership Academy must have an educational purpose and comply with student behavior guidelines.

Acceptable uses for students include:

- Visiting websites or databases that pertain to classroom activities or lessons.
- Creating or maintaining school or individual web pages or conducting email communications, all under the direction of staff.
- Using search engines to access information, websites, or pictures that pertain to classroom material or projects.

IV. Unacceptable Uses

The transmission of materials that violate state/federal law or Riverside Leadership Academy policy is strictly prohibited.

Unacceptable uses include, but are not limited to:

- Taking any actions that may disrupt the Riverside Leadership Academy network; this includes knowingly introducing a virus and “hacking”.
- Disclosing, using, or disseminating personal information about any minor on the Riverside Leadership Academy network.
- Accessing threatening or obscene materials.
- Using language that threatens another individual.
- Violating copyright laws and/or clickable licensing agreements.

- Accessing personal email accounts or other forms of direct electronic communication including chat rooms for non-educational purposes.
- Using the name and password of another user.

Additionally, students may not use personal cellular connections to access the internet while on Riverside Leadership Academy campus. All student access to the internet must be via Riverside Leadership Academy's network.

V. Staff Responsibilities

It is the responsibility of Riverside Leadership Academy staff members who have direct contact with students to educate students on online safety and cyberbullying prevention. Education related to online safety and cyberbullying prevention may include in-class discussions and assignments, webinars, parent meetings, or online courses. Riverside Leadership Academy staff members are also responsible for supervising students during class time internet use.

VI. Student Responsibilities

It is the responsibility of Riverside Leadership Academy students to abide by the school AUP and participate in online safety education offered by the school.

VII. Safety and Ethical Use

Any internet user must take reasonable precautions to protect him or herself online. Students, staff, and visitors should use the guidelines listed in this section.

VIII. Email, Forums, Instant Messaging, and Other Online Messaging

Never share personal information online. This includes, but is not limited to: real full name, postal address, social security number, and passwords. Sharing the information of another individual, especially minors, is unethical, strictly forbidden by the AUP, and may be unlawful. In the case of students, the privacy of student educational data is protected by the Family Educational Rights and Privacy Act (FERPA). When in doubt, do not release student data and consult a school administrator for further advice.

Special care must be taken when sending mass emails. Email addresses themselves are private information, and improper mass emailing can result in inadvertent sharing of addresses. Improper mass emailing can also allow recipients to reply to the mass message and send their own messages to the entire group. This is preventable by using a blind carbon copy (Bcc) feature or a mass emailing service. It is the responsibility of all Riverside Leadership Academy staff and students to use Bcc or a mass emailing service and to protect private information and data when sending mass emails.

IX. Unauthorized Access / Hacking and General Unlawful Activity

Gaining or attempting to gain unauthorized access to Riverside Leadership Academy resources, or using Riverside Leadership Academy resources to gain or attempt to gain unauthorized access to outside systems is unethical, unlawful, and forbidden by the AUP. This includes bypassing the internet filter without permission or purposefully gaining access to material that is harmful to minors. Assuming the online identity of another individual for any purpose is unethical and forbidden. Use of Riverside Leadership Academy resources for any unlawful purpose, including, but not limited to, copyright infringement, is unethical and forbidden by the AUP.

X. Academic integrity

Students are expected to follow all Board and school handbook policies regarding academic integrity when using technology.

XI. Harassment and Cyberbullying

Cyber bullying may involve any of these behaviors:

- Accessing, producing, posting, sending, or displaying material that is offensive in nature on the internet.
- Harassing, insulting, or attacking others on the internet.
- Posting personal or private information about other individuals on the internet.
- Posting information on the internet that could disrupt the school environment, cause damage, or endanger students or staff.
- Concealing one's identity in any way, including the use of anonymization tools or another individual's credentials/online identity, to participate in any of the behaviors listed above.

The Executive Director will determine whether or not specific incidents of cyberbullying have impacted the school's climate or the welfare of its students and appropriate consequences will be issued.

Schools are not responsible for electronic communication that originates off-campus.