INTERNET SAFETY AND TECHNOLOGY

The Rutherford Board of Education is committed to effectively using technology to advance and promote learning and teaching. Educational technology shall be infused into the district curriculum to maximize student achievement of the Common Core State Standards and the NJ Core Curriculum Content Standards.

It is the policy of the district to establish safe and effective methods for student and staff users of the district's technological resources and to:

A. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

B. Prevent unauthorized access and other unlawful online activity;

C. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

D. Comply with the Children's Internet Protection Act (CIPA).

COMPLIANCE WITH CIPA

Filters Blocking Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet or other forms of electronic communications from access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.
Technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. Students are expected to respect the filter as a safety precaution and shall not attempt to circumvent the web filter.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the school district online computer network.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

A. Unauthorized access, including so-called "hacking," and other unlawful activities; and

B. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the school district staff to educate, supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Procedures for the disabling or otherwise

INTERNET SAFETY AND TECHNOLOGY

modifying any technology protection measures shall be the responsibility of the chief school administrator or his or her designee.

The chief school administrator or his or her designee shall ensure that students who use the school internet facilities receive appropriate training including the following:

A. The district established standards for the acceptable use of the internet;

B. Internet safety rules;

C. Rules for limited supervised access to and appropriate behavioral expectations for use of online resources, social network websites, and chat rooms;

D. Cyberbullying (board policy 5131.1 Harassment, Intimidation and Bullying) awareness and response.

Students are responsible for maintaining appropriate behavior on all school computers and the school network. Users must maintain high standards of ethical conduct while using the network. Employees are not to engage in any behavior that brings embarrassment, harm, or otherwise detracts from the good reputation of the Rutherford School District, its staff and students.

ACCEPTABLE USE OF THE INTERNET

Purpose

To support its commitment to providing avenues of access to the universe of information available, the district shall provide access to the Internet.

Limitation of Liability

The Internet constitutes an unregulated collection of resources that changes constantly, so it is not possible to totally predict or control the resources that users may locate. The board cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the board be responsible for financial obligations arising through the unauthorized use of the system.

District Rights and Responsibilities

The computer system is the property of the district, and all computer software and hardware belong to it. Therefore, the district retains the right to monitor all access to and use of the Internet.

The board designates the chief school administrator as the coordinator of the district system. He/she shall recommend to the board of education qualified staff persons to ensure system integrity and coordinate other activities as required to maintain the system.

Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Any type of information stored on district electronic devices becomes the property of the Rutherford School District. The Rutherford School District can periodically review and monitor all files and data stored on district electronic

INTERNET SAFETY AND TECHNOLOGY

devices. The Rutherford School District can edit or remove any material, which the system administrators, in their sole discretion, believe to be inappropriate. Access to and review of such files is not limited to probable cause. Privacy is neither implied nor granted, nor should it be expected.

Access to the System

This acceptable use policy shall govern all use of the system. Sanctions for student misuse of the system shall be included in the disciplinary code for students, as set out in regulations for policy 5131 Conduct/Discipline. Employee misuse many result in appropriate discipline in accord with the collective bargaining agreement and applicable laws and regulations.

The board shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

Student Safety Practices

Students shall not post personal contact information about themselves or others. Nor shall students engage in any kind of personal contact with individuals they meet online. Attempts at contact from such individuals should be reported immediately to the staff person monitoring that child's access to the Internet.

Prohibited Activities

Users shall not attempt to gain unauthorized access (hacking) to the district system or to any other computer system through the district system, nor shall they go beyond their authorized access. This includes attempting to log in through another individual's account or accessing another's files.

Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, "Trojan Horses," trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

Users shall not use the district system to engage in illegal activities.

Users shall not access material that is profane or obscene, that advocates illegal acts, or that advocates violence or hate. Inadvertent access to such material should be reported immediately to the supervising staff person.

Users shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own.

Users shall not infringe on copyrighted material and shall follow all dictates of copyright law and the applicable policies of this district.

Users shall not attempt to circumvent the district security and content filters by any means, including proxy servers.

Users shall not distribute any commercial, political, or religious material.

INTERNET SAFETY AND TECHNOLOGY

Users shall not download or play games on the Internet of a non-educational nature.

Users shall not employ the network for commercial purposes and personal or financial gains.

Users shall not connect personal electronics to the network.

Users shall not harass, insult or attack others or engage in any type of cyberbullying.

Prohibited Language

Prohibited language applies to public messages, private messages, and material posted on web pages.

Users shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language.

Users shall not use the system to spread messages that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security

Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or data processing department if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.

Users shall not install or download software or other applications without permission of the supervising staff person.

Users shall follow all district virus protection procedures when installing or downloading approved software.

System Limits

Users shall access the system only for educational activities.

Designation of quotas for disk usage on the system may be established and users must respect these system limitations.

Privacy Rights/Personal Safety

Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.

Users shall not publish private information about another individual.

Students should never share personal information, such as phone number, address, social security number, birthday, or financial information over the Internet. Communicating over the

INTERNET SAFETY AND TECHNOLOGY

Internet brings anonymity and associated risks, and students should carefully safeguard the personal information of themselves and others.
Students should never agree to meet someone they meet online without parental permission. If a student sees a message, comment, image, or anything else online that makes him/her concerned for his/her personal safety, this should immediately be brought to the attention of a supervising teacher or staff member.

It is important to keep passwords secure and private. Users should not gain or attempt to gain unauthorized access to District Technology, or that of another individual. This includes going beyond authorized access, attempting to log in through another person's account, impersonating another individual or a fictional individual online, and accessing another person's files.

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use trusted sources when conducting research via the Internet. Users should be aware that once something is online it can be shared and spread in ways the student never intended.

School Furnished Electronic Devices

The district may furnish students with electronic devices such as laptop computers, tablets, notebooks, cellular telephones, or other electronic devices to use outside of school. When a student is furnished with an electronic device to use outside of school, the district shall provide the student with written or electronic notification that the device may record or collect information on the student's activity or the student's use of the device if the electronic device is equipped with a camera, global positioning system, or other feature capable of recording or collecting information on the student's activity or use of the device. The notification shall also include a statement that the district shall not use any of the capabilities in a manner that would violate the privacy rights of the student or any individual residing with the student. The parent or guardian of the student furnished with an electronic device shall acknowledge receipt of the notification. The district shall retain the acknowledgement for as long as the student retains the use of the device.

Implementation

The chief school administrator may prepare regulations to implement this policy.

Adopted: July 9, 2001
Renumbered: 07/12/04 (5512)
Revised: July 9, 2007
Revised: November 8, 2010
Revised: May 14, 2012
Revised: November 10, 2014
Renewed: July 18, 2016

Legal References:	N.J.S.A. 2A:38A-1 et seq.	Computer System
	N.J.S.A. 2C:20-25	Computer Related Theft
	N.J.S.A. 18A:7A-10 et seq.	New Jersey Quality Single Accountability Continuum for evaluating school performance
	N.J.S.A. 18A:36-35	School Internet websites; disclosure of

INTERNET SAFETY AND TECHNOLOGY

	certain student information prohibited
N.J.S.A. 18A:36-39	Notification by school to certain persons using certain electronic devices; fine
N.J.A.C. 6A:30-1.1 et seq.	Evaluation of the Performance of School Districts
17 U.S.C. 101	United States Copyright Law
47 CFR 54.503(d)	Competitive Bidding; Gift Restrictions
47 U.S.C. 254(h)	Children's Internet Protection Act

State in re T.L.O., 94 N.J. 331 (1983), reversed on other grounds, New Jersey v. T.L.O., 569 U.S. 325 (1985).

O'Connor v. Ortega 480 U.S. 709 (1987)

No Child Left Behind Act of 2001, PL 107-110, 20 U.S.C.A. 6301 et seq.