INTERNET SAFETY AND TECHNOLOGY/ ACCEPTABLE USE POLICY

The Passaic Board of Education shall develop a technology plan that promotes the effective use of electronic communication to advance and promote learning and teaching. Educational technology shall be infused into the district curriculum to maximize student achievement of the New Jersey Student Learning Standards for all content areas and grade levels. 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).

Purpose

Passaic Public Schools will support its commitment to providing reliable and safe access to the Internet for students and staff.

Limitation of Liability

The Internet constitutes an unregulated collection of resources that change 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, including hardware and software, is the property of the Passaic Public Schools. Therefore, the district retains the right to monitor all access to, and use of, the Internet. The Board designates the Superintendent as the coordinator of the district system. The Superintendent or his/her designee shall recommend to the Board of Education qualified staff persons to ensure provision of accounts necessary for access to the Internet, establishment of a virus protection process, and coordination of other activities as required to maintain the system. The district will work to ensure that teachers and staff receive proper training in the use of the system; ensure that students are adequately supervised when using the system; and maintain

executed user agreements. The district shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

Access to the System

This acceptable use policy shall govern all use of the information system. All students and employees of the Passaic Public Schools shall have access to the Internet through the district's network with a signed agreement (see Exhibits A and B). To deny a child access, parents/guardians must notify the building principal in writing.

There will be sanctions for student and staff misuse of the system as set out in the Acceptable Use for Technology Regulation. The board shall adopt the following standards of conduct for the use of computer network/computers including electronic mail communications (see also Exhibit B). All student and staff users of school computer networks/computers shall adhere to the board standards of acceptable use of technology, as defined in this policy. Violation of the board policy for acceptable use may result in disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The board shall provide access to school computer networks/computers for educational purposes only, and, for employees, for purposes related to job performance. The board retains the right to restrict or to terminate access to the computer network/computers at any time, for any reason. The board retains the right to have district personnel monitor network activity, in any form necessary, to maintain the integrity of the network and to ensure its proper use and compliance with federal and state laws that regulate Internet Safety. Access to the district network/computers is a privilege.

For the purpose of this policy, the following definitions shall apply:

A. Computer Network/Computers
   "Computer network/computers" consist of any school managed or owned computer equipment or systems, including, but not limited to, networks, hard drives, servers, peripherals, printers, networking systems, tablets, electronic devices, laptops/chromebooks, modems, electronic documents, applications or apps, video, voice and data networks, routers, storage devices, and classrooms equipped with such equipment. "Computer network/computers" shall also include electronic communications which shall be defined as and include the use of information systems in the communicating, posting, or obtaining of information or materials by ways of electronic mail, chats/forums, messaging, bulletin boards, Internet, or other such electronic tools.

B. User
A "user" is any individual, with or without authorization, who utilizes the board's computing system from any location.

Compliance with Children's Internet Protection Act (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 communications, or other forms of electronic communications. Specifically, as required by the Children's Internet Protection Act (CIPA), blocking shall be applied to any depiction of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. Such requests must be in writing to the appropriately identified administrator.

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 when using electronic mail, instant messaging, and other forms of direct electronic communications. 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 modifying any technology protection measures shall be the responsibility of the Superintendent or his or her designee.

The Superintendent or his or her designee shall ensure that students and staff 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, and social network websites; and
D. Cyberbullying (board policy 5131.1 Harassment, Intimidation and Bullying) awareness and response.

Individual Google Apps Accounts for Students

Students in grades K-12 are provided with an individual Google Apps account. An individual account for any such student shall require an Acceptable Use Agreement signed by the student and his/her parent/guardian (see Exhibit B). Email may be added to a student's Google Apps account in grades 9-12. An individual account for any such student shall require an agreement signed by the student and his/her parent/guardian (see Exhibit B). The district retains the right to access all materials shared through such an account and the right to delete accounts and their contents.

Supervision of Students

Student use of the Internet shall be supervised by qualified staff.

District Website

The Board authorizes the Superintendent or his/her designee to establish and maintain a district website. The purpose of the web site will be to inform the district educational community of district programs, policies, and practices.

The Superintendent or his/her designee shall ensure that district and school websites do not disclose photos or personal information about students without prior written consent from parents/guardians. Consent shall be obtained on Exhibit 5145.5.

Acceptable Use of District Network and Computers

The Passaic Board of Education recognizes new technologies may shift the manner in which information is accessed, communicated, and transferred; these information and communication technologies will alter and enhance the nature of teaching and learning. The board supports access by students and employees to such information sources to create a 21st century learning experience that adequately prepares them for college and career. The board also reserves the right to limit use of these technologies on the computer network to legitimate, appropriate educational purposes.

The board supports users utilizing the computer network in a manner that is responsible, ethical, respectful, and in accordance with this policy and law. The district will make a reasonable effort to monitor the use of school computer networks/computers and internet filters shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

All users are responsible for appropriate use of the district's technological resources, which include the network, computer labs, hardware peripherals, audio-visual systems, digital boards, communication systems, databases, etc.

Student Safety Practices

Students shall not post personal information about themselves or others nor shall students engage in any kind of personal contact with individuals they meet online while on school premises or using school hardware or software applications, or using district provided internet access. Posting contact information about students, including students' own contact information is prohibited. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

Prohibited Activities

Users shall not attempt to gain unauthorized access 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 person's files. Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, malware, "Trojan Horses," or any similar products 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. When using information found online, students and staff should cite the original author.

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

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

All users of district computers must have their own unique password which may not be shared with anyone. If an employee believes that their password has been lost or stolen or that the network has been accessed by someone without authorization, he/she must contact the district Help Desk to report the issue immediately. All suspicious activity on the district network, such as phishing emails or "spam", must also be reported to the district Help Desk.

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 district Help Desk if they detect a possible security problem. Users shall not install or download software or other applications without permission of the Division of Information Technology. Users shall follow all district virus protection procedures when installing or downloading approved software. All computer terminals must be locked or logged off when away from desks during the day and logged off each night.

Privacy Rights

Users shall be aware that there is no expectation of privacy with district network and computers. Users shall not publish private information about another individual. District databases that secure information about academic life, community members, and school business are the property of the district. Information contained therein is confidential and can neither be distributed nor used for personal gain. The district reserves the right to restrict access to such databases.

In accordance with N.J.S.A. 18A:36-39 students furnished with a computer, laptop, or other electronic device are hereby notified that the electronic device may record or collect information on the student activity or student use of the device. Collection of this information will not be used in a manner that would violate the personal privacy rights of the student or any individual residing with the student. When a student is furnished with an electronic device, the district shall provide the student with written or electronic notification that the electronic 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 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 an electronic device shall acknowledge receipt of the notification. The district shall retain the acknowledgment as long as the student retains the use of the electronic device. Failure to provide the required notification shall be subject to a fine of $250 per student, per incident (Exhibit B).

Users' files and other electronic storage areas shall be considered district property for purposes of inspection and control. The system administrator may access all such files and communications. Users are informed by the Acceptable Use Policy (Exhibit A and B) that any information stored is not private. Individuals should have no expectation of privacy with respect to their files or communications on board provided computer network/computers. All data stored or transmitted or accessed by users, including email, online forums, and messaging can and will be monitored by the board.

It is expressly understood that the system administrator may monitor staff/student activity on the networks/computers and the Internet and may access any files stored by user on district computers or at a remote site accessed by district computers. It is further understood that the Superintendent or his/her designee may discontinue the networks/computers and Internet access privileges and student discipline will be administered following Policy No.5131.

Standards for Use of Computer Networks

District network services and devices are provided exclusively for informational and educational purposes. Educational purposes are those that are related to or necessary to complete lessons or classroom assignments, and, for employees, those purposes related to job performance. Users will comply with district standards, federal and state laws, and will act in a responsible and legal manner. Users are prohibited from engaging in the following conduct and shall be subject to discipline and/or legal action for such conduct:

A. Using the network and/or computers for other than educational purposes;
B. Using the network and/or computers for illegal activities or in support of illegal activities. Illegal activities are defined as activities which violate federal, state, and local laws or regulations;
C. Using the network and/or computers in a way that violates existing board policy;
D. Using the network and/or computers for obscene purposes or to obtain or transmit obscene materials. Obscene materials are those that appeal to the prurient interest and/or depict sexual conduct in an offensive way;
E. Using the network and/or computers to send or display lewd, indecent, or vulgar speech or materials;
F. Using the network and/or computers to send or display harassing, demeaning, or offensive speech or materials;
G. Using the network and/or computers to engage in activities that could materially or substantially interfere with the operation of the school, the school's educational mission, or other students' rights;
H. Using the network and/or computers to violate copyrights, trademarks, an individual's right of publicity, any form of intellectual property, license agreements, or other contracts;

I. Connecting personal devices or equipment (including personal cellular device) to the physical district network without prior permission;
J. Using the network and/or computers in a manner that:
    1. Intentionally disrupts network traffic or crashes the network;
    2. Degrades or disrupts equipment or system performance. Examples of conduct that degrade or disrupt equipment or system performance include, but are not limited to, the following activities: installing computer viruses; disabling protective software; sending unnecessary or excessive mail or messages; causing denial-of-service attacks and others.
    3. Uses the computing resources of the district for commercial purposes, financial gain, or fraud;
    4. Steals data or other intellectual property;
    5. Gains or seeks unauthorized access to files of others or vandalizes the data of another user;
    6. Forges electronic mail messages or uses an account owned by others;
    7. Invades the privacy of others. Users will not use the network to obtain private information about others, post private information about another person, or re-post a message that was sent to them privately without permission of the person who sent the message;
    8. Disrupts the learning process by engaging in the playing of online games that are not intended for educational purpose or academic gain;
    9. Violates the safety and security of others or is disrespectful to others by using language that includes but is not limited to profane, racist, sexist, or discriminatory remarks; or any violation of the HIB policy;
    10. Possesses any data which is in violation of this policy; and/or
    11. Engages in other activities that do not advance the educational purposes for which the computer network/computers are provided.

Violation of Acceptable Use Policy

The use of the Internet is a privilege. Any violation of board policy may result in the loss of district provided access to technology. Law enforcement agencies may be contacted regarding potential illegal activities. Users in violation of this policy are subject to the following consequences, which include but are not limited to:

A. Use of computer networks/computers only under direct supervision;
B. Limited access to predetermined educational resources;
C. Suspension and/or revocation of network privileges and/or computer privileges under extreme circumstances;
D. For employees: letters of reprimand, increment withholding, loss of employment;
E. Legal action and prosecution by the appropriate authorities.

Standards for the Promotion of Online Safety for Students

Students are required to adhere to the following guidelines regarding safety. Any individual who fails to adhere to these guidelines may have his/her network privileges revoked:

A. Users are prohibited from displaying any personally identifiable information about students including name, address, photographs, social security number, or other personal characteristics that would make the student easily identifiable without obtaining prior consent of the student's parent or guardian;
B. Students are obligated to disclose to a teacher or parent any information or electronic messages which make them uncomfortable;
C. Students shall never engage in any kind of personal contact or meet with individuals they meet online without first receiving permission from a parent. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs;
D. Users should never divulge their district-assigned credentials (username/password) and will be held accountable for the consequences of intentionally or negligently disseminating this information.

Parental Notification and Responsibility

The superintendent or his/her designee shall ensure that parents/guardians are notified about the district network and the rules governing its use. Parents/guardians shall sign and return Acceptable Use Agreement Parent and Student (Exhibit B), to allow their child(ren) to have an individual account. Parents/guardians who do not wish their child(ren) to have access to the Internet must identify this when completing Exhibit B.

Due Process

In the event there is an allegation that a student has violated the Acceptable Use Policy, that student will be provided with a written notice of the alleged violation and an opportunity to present an explanation before a district administrator. Employee violations of the Acceptable Use Policy will be handled in accordance with board policy and the current Collective Negotiations Agreement.

Responsibility for Damage Suffered

The board makes no warranties of any kind, expressed or implied, for the Internet access it provides. The board will not be responsible for any damage users suffer including, but not limited to, loss of data or interruption of service. The board is not responsible for the accuracy or quality of the information obtained through or stored on the system. The board is not responsible for financial obligations arising from the unauthorized use of the system.

Specific conditions and services on the computer network and the Internet change from time to time, and the board makes no warranties with respect to services and specifically assumes no responsibility for:

A. Any costs, liability, or damages caused by staff/student use of the computer networks or the Internet;
B. Any consequences of service interruptions or changes whether or not they were under the control of school district staff; and/or
C. Users will be personally charged for any unauthorized costs incurred in their use of the computer network/computers and held responsible for any damages caused by their misuse of the computer network/computer equipment.

The board will fully cooperate with any local, state, or federal agency in any investigation concerning or relating to misuse of the board's computer network/computers.

First Reading: December 19, 2016
Second Reading: January 30, 2017
Adopted: January 30, 2017

First Reading: July 29, 2019
Second Reading: August 28, 2019
Readopted: August 28, 2019

Legal References:

N.J.S.A. 2A:38A-1 et seq.	Actions for computer related offenses
N.J.S.A. 2C:20-25	Computer criminal activity; degree of crime; sentencing
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 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)

Every Student Succeeds Act of 2015, Pub. L. 114-95, 20 U.S.C.A. 6301 et seq.

Possible

Cross References:

*1111	District publications
*3514	Equipment
3543	Office services
*3570	District records and reports
4118.2/4218.2	Freedom of speech (staff)
*5114	Suspension and expulsion
*5124	Reporting to parents/guardians
*5131	Conduct/discipline
*5131.5	Vandalism/violence
*5142	Pupil safety
5145.2	Freedom of speech/expression (students)
*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.