2361 ACCEPTABLE USE OF COMPUTER NETWORKS/ COMPUTERS AND RESOURCES

The Board shall develop a technology plan that effectively uses electronic communication to advance and promote learning and teaching. This system of technology shall be used to provide local, Statewide, national and global communications opportunities for staff and students. Educational technology shall be infused into the district curriculum to maximize student achievement of the 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 including pornography, electronic mail, or other forms of direct electronic communications or material meeting the criteria of HIB;

B. Prevent unauthorized access and other unlawful online activity;

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

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, chat rooms, 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 technology;

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 awareness and response.

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

Acceptable Use of Technology

Purpose

To support its commitment to providing avenues of access to the universe of information available, the district's system of electronic communication shall include 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 IT System and its components and data 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 Superintendent as the coordinator of the district system. He or she shall recommend to the Board of Education qualified staff persons to ensure supervision of individual and class accounts necessary for access to the Internet, designation of quotas for disk usage on the system, establishment of a document retention schedule, establishment of a virus protection process and coordination of other activities as required to maintain the system.

The Principal shall coordinate the district system in his or her building by approving all activities for that building; ensuring that teachers receive proper training in the use of the system; ensuring that students are adequately supervised when using the system; maintaining executed user agreements; and interpreting this Acceptable Use of Technology Policy at the building level.

Access to the System

This Acceptable Use of Technology 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 Board policy.

Conduct and Discipline

Employee misuse may 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 and filtering software to deny access to certain areas of the Internet.

World Wide Web

All students and employees of the Board shall have access to the Web through the district's networked or stand-alone computers and other devices. An agreement shall be required. To deny a child access, parents or guardians must notify the Building Principal in writing.

Individual E-mail Accounts for Students

Students in grades five through eight may be granted individual accounts at the request of teachers and with the consent of parents or guardians. An individual account for any such student shall require an agreement signed by the student and his or her parent or guardian.

Individual E-mail Accounts for district Employees

District employees shall be provided with email access. Access to the system will be provided for staff members who have signed the Acceptable Use of Technology Policy agreement. Email will be monitored as deemed necessary by the administration. Employee email is discoverable and will be released if subpoenaed within the archival period set forth in this policy.

District Website

The Board authorizes the Superintendent to establish and maintain a district website. The purpose of the website will be to inform the district educational community of district programs, policies and practices.

Classes may also establish websites that include information on the activities of that school or class. The Building Principal shall oversee these websites.

The Superintendent shall publish and disseminate guidelines on acceptable material for these websites. The Superintendent shall also ensure that district and school websites do not disclose personally identifiable information about students without prior written consent from parents or guardians. Consent shall be obtained on the form developed by the State Department of Education. "Personally identifiable information" refers to student names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

Parental Notification and Responsibility

The Superintendent shall ensure that parents or guardians are notified about the district network and the rules governing its use. Parents or guardians shall sign an agreement to allow their child(ren) to have an individual account. Parents or /guardians who do not wish their child(ren) to have access to the Internet must notify the Principal in writing.

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 shall be reported immediately to the Superintendent or his or her designee. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

Prohibited Activities

A. 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.

B. 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.

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

D. 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.

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

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

G. Users shall not engage in any action that violates existing Board policy or public law.

H. Users shall not access chat rooms, sites selling term papers, book reports and other forms of student work.

I. Users shall not access messaging services (i.e. MSN Messenger, ICQ, etc.).

J. Users shall not access internet and/or non-academic computer games.

K. Users shall not download outside data disks or external attachments without prior approval from the administration.

L. Users shall not change the computer setting (exceptions include personal settings such as font size, brightness, etc.).

M. Users shall not download unauthorized applications.

N. Users shall not send spam — sending mass or inappropriate emails.

O. Users shall not access the school's Internet or email accounts for financial or commercial gain or for any illegal activity.

P. Users shall not send of anonymous and/or false communications such as MSN Messenger, Yahoo Messenger.

Q. Users shall not give out personal information, for any reason, over the Internet. This includes, but is not limited to, setting up Internet accounts including those necessary for chat rooms, eBay, email, etc.

R. Users shall not participate in credit card fraud, electronic forgery or other forms of illegal behavior.

S. Users shall not bypass the school web filter through a web proxy.

Prohibited Language

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

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

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

System Security

A. 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 or her password to another individual.

B. Users shall immediately notify the Superintendent or his or her designee if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.

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

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

System Limits

A. Users shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists, instant message services and participation in Internet "chat room" conversations.

B. Users shall check e-mail frequently and delete messages promptly.

Privacy Rights

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

B. Users shall not publish private information about another individual.

School Furnished Electronic Devices

The district may furnish students with electronic devices such as laptop computers, tablets, notebooks, or other electronic devices. 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 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 as long as the student retains the use of the electronic device.

Parent or Guardian Responsibilities

A. Parents or guardians agree to discuss the values and the standards that the child(ren) should follow on the use of the Internet just as you do on the use of all media information sources such as television, telephones, movies, and radio.

B. Parents or guardians wishing to opt out of having the child(ren) assigned a school furnished electronic device, shall submit a signed letter indicating this, stating the reason(s) why. Students not using a school furnished electronic device are responsible for meeting the course requirements.

School Responsibilities

A. School will provide Internet and email access to its students.

B. School will provide Internet blocking and/or filters as necessary during the school day and whenever students are using the district website, for the prevention of access to inappropriate materials.

C. School will provide network data storage areas. These will be treated similar to school lockers. The school district reserves the right to review, monitor, and restrict information stored on or transmitted via school owned equipment and to investigate inappropriate use of resources.

D. School will provide staff guidance to aid students in doing research and help assure student compliance of the Student Code of Conduct Policy.

E. School will provide any student appropriate substitute material if privilege of technology is revoked.

Student Responsibilities

A. Students will use computer/devices in a responsible and ethical manner.

B. Students will obey general school rules concerning behavior and communication that apply to computer use.

C. Students will use all technology resources in an appropriate manner so as not to damage school equipment. This "damage" includes, but is not limited to, the loss of data resulting from delays, non-deliveries, miss-deliveries or service interruptions cause by the student's own negligence, errors or omissions. Use of any information obtained via the school district's designated Internet system is at your own risk. The school district specifically denies any responsibility for the accuracy or quality of information obtained through its services.

D. Students will help the school district protect its computer system/devices by contacting an administrator about any security problems they may encounter.

E. Students will monitor all activity on their account(s).

F. Students should always turn off and secure their computer after they are done working to protect their work and information.

G. If a student should receive email containing inappropriate or abusive language or if the subject matter is questionable, he or she is asked to print a copy and turn it in to the office.

H. Students will return their computer to the Watchung Borough School District at the end of each school year. Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment at school for any other reason must return their school furnished electronic device on the date of termination.

I. Student will be responsible for completing course work if technology privilege is revoked.

Care

Students will be held responsible for maintaining their individual computers and keeping them in good working order. Students will be responsible for damages to their computers:

A. The computer batteries must be charged and ready for school each day.

B. Only labels or stickers approved by the Watchung Borough School District may be applied to the computer.

C. The computer cases furnished by the school district must be returned with only normal wear and no alterations to avoid paying a protective case replacement fee.

D. School issued computers that malfunction or are damaged must be reported to the school office. The school district will be responsible for repairing computers that malfunction. Computers that have been intentionally damaged from student misuse or neglect will be repaired with the cost being borne by the student's parent or guardian. Student's parent or guardian will be responsible for the entire cost of repairs to computers that are damaged intentionally or be responsible for full replacement cost.

E. School issued computers that are stolen or lost must be reported immediately to the office and the police department.

Legal Propriety

A. Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If unsure, ask a teacher or parent or guardian.

B. Plagiarism is a violation of the student handbook. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.

C. Use or possession or hacking software is strictly prohibited and violators will be subject to disciplinary action. Violation of applicable State or Federal law will result in criminal prosecution and/or disciplinary action by the district.

Student Discipline

If a student violates any part of the above policy, he or she will be subject to consequences as listed in the Student Code of Conduct Policy.

Implementation

The Superintendent may prepare regulations to implement this policy.

N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act
Federal Communications Commission: Neighborhood Children's Internet Protection Act

Adopted: 25 April 2018