WASHINGTON ACADEMY
BOARD POLICY

2090

TECHNOLOGY/INTERNET USE AND SAFETY POLICY

The Board of Directors has approved the following Technology/Internet Use and Safety Policy to provide access to technology and the internet in the school building to promote 21st Century skills development.

This policy covers both Staff and students.

As outlined in the NJ C.C.C.S. and Washington Academy's curriculum maps, technology is integrated throughout the curricular content areas to foster student learning and growth as well as prepare them for the 21st Century jobs. In addition, the school has provided technology to Staff to research, organize and adequately plan lessons that incorporate technology with a robust hands-on learning model.

The following goals support the purpose of the policy:

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).

CIPA (Children's Internet Protection Act)Compliance

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 (CIPA), 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. It is Washington Academy policy that any student or Staff Member that attempts to by-pass, thwart, disable or use proxies to undermine or go around such Internet filters is a violation of school policy and shall be subject to disciplinary action and may result in the loss of privileges to technology or internet usage.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the school 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 (CIPA), 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 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 (CIPA). Procedures for the disabling or otherwise 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 and staff who use the school Internet facilities receive appropriate training including the following:

A. The school established code of acceptable use of the internet and online conduct;
B. Rules for limited supervised access to and appropriate behavioral expectations for use of online resources, social network websites, and chat rooms;
C. Cyber bullying awareness and response (B.P. 4060) Student use of the Internet shall be supervised by qualified staff.

Washington Academy Rights and Responsibilities

The computer system is the property of the Washington Academy, and all computer software and hardware belong to it. Therefore, the school retains the right to monitor all access to and use of the Internet. The Board of Directors designates the Chief School Administrator as the coordinator of the district system. He/she shall recommend to the Board of Directors qualified staff persons to ensure provision 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 Chief School Administrator or his or her designee shall approve all activities in the school; ensure that teachers receive proper training in the use of the system; ensure that students are adequately supervised when using the system; maintain executed user agreements; and interpret this acceptable use policy.

Access to the System

This 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 outlined in the Student Handbook.

Staff Member misuse may result in appropriate discipline in accord with applicable laws and regulations. The Board of Directors shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

World Wide Web Access and User Agreement

The computers and other hardware may be capable of accessing the W.W.W. and thus all internet users must agree to a User Agreement prior to being given access to the internet. Students must sign the agreement per school year, but Staff only need to sign one (1) User Agreement during their employment at Washington Academy.

Washington Academy has the right to change, modify or alter the User Agreement, in which case, all Staff Members would need to read, review and agree to the new User Agreement.

It should be noted that use and access of computer/technology hardware, software and access to the internet is a privilege, not a right, and Washington Academy has no established policy that guarantees any student or Staff Member required access to technology or the internet in order to fulfill grade level standards for academic promotion, or to access NJ's Common Core Standards to research and prepare lesson plan. If a student or Staff Members computer, technology or internet privileges have been revoked or modified in any way, the school shall provide hard copies of all material that would otherwise be accessed online or through the internet.

Violation of the user agreement or this *Technology/Internet Use and Safety Policy* by a student or Staff Member may result in revoked, denied, modified, or limited privileges and/or may also be subject to disciplinary action, which may include student suspension or for Staff Members cause for termination of employment.

A parent or legal guardian may exercise his/her right to deny his/her own child's computer, technology or internet privilege at any time, by notifying the Principal in writing.

Parental Notification and Responsibility

Annually, the school shall send the User Agreement and the Student Handbook, which includes the code of student conduct. Parents/legal guardians shall sign the User Agreement on behalf of his/her minor child, or for a student who has reached the age of majority, may sign in conjunction with his/her child.

Classroom E-mail, Web 2.0, and Social Network Accounts

In order to access some software and technology, the school may set up user accounts for students, which require log-in names and passwords. In some cases, the school shall provide this user info to parents, legal guardians and students for universal access.

Staff Members have user accounts created with his/her name and a password, which is recorded in the school IT database. If a Staff Member needs to change a password, or cannot access his/her accounts for any reason, he/she should notify the IT Administrator immediately for further technical support.

Individual E-mail, Web 2.0, and Social Network Accounts for Staff Members

Staff Members who have signed the User Agreement shall be provided a school email account and access to other software, hardware and online accounts. All emails will be monitored and archived for three years. Staff Member email is discoverable and will be released if subpoenaed within the archival time period established in this policy. Staff Members shall be granted access to Web 2.0 and educational social network services to support the delivery of instruction and implementation of the Common Core State Standards (CCS) for mathematics and language arts and literacy as well as the New Jersey Core Curriculum Content Standards (NJCCCS). Staff Members must use these services in accordance with school policies and regulations.

Students and Staff Members who misuse the aforementioned technology resources and violate the policies and regulations outlined by the Washington Academy Board of Directors will forfeit the right to access these resources and, if necessary, face disciplinary action.

School Web Site

The Board of Directors authorizes the Chief School Administrator to establish and maintain a school web site. The purpose of the web site will be to inform the school educational community of school programs, policies and practices and to conform to NJ State code and regulations.

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 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.

Cyber Bullying

Students and Staff Members shall not harass, intimidate, or bully others using electronic communications. Cyber bullying is the willful use of cell phones, computers, and other electronic communication devices to harass or threaten others. The term “cyber-bullying " shall mean any form of harassment, intimidation or bullying, as defined by HIB Policy (B.P. 4060) which is published on the school’s website and in the Student Handbook.

Prohibited Activities

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

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 IT Administrator 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, professional or career development activities. This applies to discussion group mail lists, instant messaging services and participation in “chat room” conversations or social networking environments.

Privacy Rights

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.

Surveys

As per state statute (N.J.S.A. 18A:36) and the School Surveys Policy (B.P. 4140), the administration of electronic or any other surveys to students or teachers must be approved by the Chief School Administrator.

School Furnished Electronic Devices

Washington Academy may furnish staff and students with electronic devices such as laptop computers, tablets, notebooks, cellular telephones, or other electronic devices. When a user is furnished with any electronic/technology device, the user shall be notified in writing that the electronic device may record or collect information on the user's activity or may record, if the electronic device is equipped with a camera, global positioning system, or other feature capable of recording or collecting information on the user's activity or use of the device.

The notification shall also include a statement that the school shall not use any of the capabilities in a manner that would violate the privacy rights of the user or any individual residing with the user.

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 of Directors cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the Board of Directors 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 of Directors be responsible for financial obligations arising through the unauthorized use of the system.

Implementation

The Chief School Administrator may prepare regulations to implement this policy.

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: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
- 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
- N.J. v. T.L.O. 469 U.S. 325 (1985)
- O'Connor v. Ortega 480 U.S. 709 (1987)

Policy Adopted: July 13, 2013

Policy Re-Adopted: August 29, 2016