INTERNET SAFETY AND TECHNOLOGY

The Mendham Borough Board of Education 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 New Jersey Student Learning 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).

The district shall ensure equal and bias-free access for all students to computers, computer classes, career and technical education programs, and technologically-advanced instructional assistance, regardless of race, creed, color, national origin, ancestry, age, marital status, affectional/sexual orientation, gender, religion, disability, English proficiency, immigration status, housing status or socioeconomic status.

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, Google Apps for Education (GAFE) document sharing, 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

INTERNET SAFETY TECHNOLOGY (continued)

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, social network websites, and chat rooms;

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

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

Policy Development

The district Internet Safety and Technology policy shall be adopted and revised through a procedure that includes reasonable public notice and at least one public hearing.

SCHOOL DISTRICT PROVIDED TECHNOLOGY DEVICES TO PUPILS

The Mendham Borough Board of Education may provide technology devices to pupils for school district authorized use only. The purpose of this policy is to establish guidelines and protocols for the issuance of these devices on a 1:1 basis for students in grades 3 - 8. Technology devices, at this time, are generally characterized, but not limited to Chromebooks.

In order to participate in the Mendham Borough School District 1:1 Chromebook program, parents and students must read and sign the Mendham Borough School District Acceptable Use Policy Information Technology Resources in the Schools form requiring them to comply with certain guidelines. This form must be reviewed and acknowledged via Genesis Parent Portal at the start of each school year.

Unintentional, accidental damages to a school district provided technology device will be repaired at no cost to the student/parent. A replacement device will be provided if possible. Repeated and/or willful damage of a school district provided technology device or the loss of a device will result in a charge for the full cost of repair or replacement device.

Students shall comply with all school district policies for the use of a school district provided technology device. A student shall be subject to consequences in the event the student violates any school district policy, including the district's Acceptable Use Policy, Pupil Code of Conduct, Harassment, Intimidation, and Bullying Policy, this policy, and/or any provision of the Mendham Borough School District Acceptable Use Policy Information Technology Resources in the Schools form.

ACCEPTABLE USE OF THE INTERNET

Purpose

To support its commitment to providing avenues of access to the universe of information available, the

INTERNET SAFETY TECHNOLOGY (continued)
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 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 and computer use.

The board designates the superintendent as the coordinator of the district system. He/she shall recommend to the board of education 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 and monitoring software.

Each principal shall coordinate the district system in his/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 policy at the building level.

Access to the System

Google Apps for Education (GAFE) shall be utilized by students and staff. The GAFE suite includes Gmail, Calendar, Drive, Docs and Sites. The GAFE suite resides online, in the Cloud enabling students and staff to productively access and share tools form any web browser through the use of any electronic device that has internet connectivity.

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 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/filtering software to deny access to certain areas of the Internet.

Internet

All students and employees of the board shall have access to the Internet through the district's networked computers, hand-held electronic devices such as iPads, notebooks and iPhones, and school furnished electronic devices. An agreement shall be required. To deny a child access, parents/guardians must notify the building principal in writing.

Policy Development

The district Internet Safety and Technology policy shall be adopted and revised through a procedure that includes reasonable public notice and at least one public hearing.

INTERNET SAFETY TECHNOLOGY (continued)

Google Apps for Education (GAFE) - Students

Students in grades K-8 shall have access and assign email accounts through GAFE with the consent of parents/guardians. An individual account for any such student shall require an agreement signed by the student and his/her parent/guardian.

Google Applications for Education (GAFE) - Employees

District employees shall have access and assigned email accounts through GAFE. Access to the system will be provided for staff members who have signed the acceptable use policy agreement. Email will be monitored and archived for seven years. Employee email is discoverable and will be released if subpoenaed within the archival period set forth in this policy.

District Web Site

The board authorizes the superintendent to establish and maintain a district web site. The purpose of the web site will be to inform the district educational community of district programs, policies and practices.

Individual schools and classes may also establish web pages that include information on the activities of that school or class. The building principal shall oversee these web sites.

The superintendent or his or her designee shall ensure that materials for publication on the district web site are reviewed and only appropriate materials are published. The superintendent shall also ensure that district web site does not disclose personally identifiable information about students without prior written consent from parents/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.

Direct Access to Student Information

Parents/guardians shall have direct access to individual student information through a parent/guardian issued password on the parent portal of the district website. Parents/guardians shall have access to only their child’s information.

Parental Notification and Responsibility

The superintendent shall ensure that parents/guardians are notified about the district network and the rules governing its use. Parents/guardians shall sign an agreement to allow their child(ren) to have access to GAFE including email. Parents/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 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.

Use of GAFE and Document Sharing

Only school related data and files shall be stored on the district network. The district assumes no responsibility for the loss, protection or restoration of personal data or files.

Materials that are subject to a copyright where the district or user does not have a license for such materials should not be stored on district resources, including hosted services/systems. Improper or unauthorized

INTERNET SAFETY TECHNOLOGY (continued)

usage of copyright material is shall be monitored and offending individuals subject to disciplinary measures.

Materials that are composed and shared by individual students and staff members as part of work, homework and other assigned duties or research, shall not be plagiarized, used to cheat or used for any other dishonest purpose.

Prohibited Activities - General

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.

File Code: 6142.10

INTERNET SAFETY TECHNOLOGY (continued)

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.

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 Technology Coordinator 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

INTERNET SAFETY TECHNOLOGY (continued)

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.

Users shall check e-mail frequently.

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.

School Furnished Electronic Devices

The district may furnish students electronic devices such as laptop computers, tablets, notebooks, iPads, cellular telephones, 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 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.

Failure to provide the required notification shall be subject to a fine of $250 per student, per incident. If imposed, the fine shall be remitted to the Department of Education, and shall be deposited in a fund that shall be used to provide laptop or other portable computer equipment to at-risk students.

Implementation

The superintendent may prepare regulations to implement this policy.

Adopted:	November 18,2014
NJSBA Review/Update:	April 2015
Readopted:	June 14, 2016
First Reading:	February 28, 2017
Readopted:	June 13,2017
Revised:	August 2018
1st Reading:	August 20, 2018
Readopted:	August 22, 2018

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Internet Safety, Technology, Web Site, World Wide Web, CIPA

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	NJQSAC
	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

INTERNET SAFETY TECHNOLOGY (continued)

N.J.A.C. 6A:30-1.1et 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
*5131.1	Harassment, intimidation and bullying
*5131.5	Vandalism/violence
*5142	Student 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.

INTERNET SAFETY TECHNOLOGY (continued)

MENDHAM BOROUGH SCHOOL DISTRICT ACCEPTABLE USE POLICY
INFORMATION TECHNOLOGY RESOURCES IN THE SCHOOLS

The school's information technology resources, including email and internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to the school's technological resources:

Respect Yourself

I will

- Show respect for myself through my actions.
- Use school-appropriate language and images on the computer.

Protect Yourself

I will

- Ensure that the information I post online will not put me at risk.
- Report any aggressive inappropriate behavior directed at me.
- Not share my password or account details with anyone else.

Respect Others

I will

- Not bully, harass or stalk other people online.
- Only go to sites that are related to my schoolwork.
- Not share my password or login.
- Only change or modify others' work with their permission.
- Only forward a private message with permission from the person who sent it.

Protect Others

I will

- Report any violations of this agreement that I observe.
- Forward only materials (including emails and images) that are appropriate.

Respect Copyright

I will

- Follow the copyright guidelines, always cite sources of ideas, interpretations, or statements.
- Request permission of owner if necessary.
- Not steal or share music or other media in a manner that violates their licenses.

Protect School Property

I will

- Not access or change any system programs or preferences.
- Not add files to the system or use peripheral devices or accessories if not authorized by a teacher.
- Not vandalize by causing physical damage, reconfiguring the computer system or destroying data.

Taking Care of Your Device

General Precautions:

INTERNET SAFETY TECHNOLOGY (continued)

- **The device is school property and all users will follow the ACCEPTABLE USE POLICY INFORMATION TECHNOLOGY RESOURCES.**
- **Cords and cables must be inserted and disconnected carefully to prevent damage to the device.**
- **Only labels/stickers applied by the technology department will be acceptable on District Chromebooks.**
- **Identification labels on Chromebooks and chargers must not be removed.**
- **Each day Chromebooks should be returned to the proper cart and plugged in for charging overnight.**
- **Any accidental damages should be reported to your teacher immediately.**

Carrying Devices and Care:

- **Students should carry devices with both hands when moving between classes with the said devices.**
- **Students should be careful placing devices in lockers and/or on desk to avoid placing too much pressure and weight on the device screen.**
- **The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure.**
    - **Do not lean on the top of the device when it is closed.**
    - **Do not place anything near the device that could put pressure on the device.**
    - **Do no place pencils, pens, etc on the keyboard inside the device.**
    - **Clean the screen with a soft, dry cloth or anti-static cloth.**
    - **Do not "bump" the device against lockers, walls, car doors, floors, etc. as it will eventually break the screen.**

Unintentional, accidental damages to a school district provided technology device will be repaired at no cost to the student/parent. A replacement device will be provided if possible. Repeated and/or willful damage of a school district provided technology device or the loss of a device will result in a charge for the full cost of repair or replacement device.

In accordance with the Anti-Big Brother Act (C.18A:36-39) all electronic device may record or collect information on the student's activity or 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. This serves as notification that the school district shall not use any of the capabilities in a manner that would violate the privacy rights of the student and any individual residing with the student. The parent or guardian of the student shall acknowledge receipt of this notification. The school district shall retain the acknowledgement as long as the student retains the use of the electronic device.

MENDHAM BOROUGH SCHOOL DISTRICT STUDENT AGREEMENT

I have read the Mendham Borough School District Rules and Responsibilities for computer use. I understand the rules and responsibilities and agree to abide by their provisions. I understand that I may use the Mendham Borough School Districts computers only if I comply with the rules and that not doing so will result in the loss of my computer access and related privileges and that I may be subject to disciplinary or legal action.

By completing this form, we agree to these terms.