

REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 1 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

2361 Acceptable Use of Computer Networks/Computers and Resources

The South Hunterdon Regional school district provides computer equipment, computer services, and Internet access to its pupils and staff, and permits the use of privately owned computer devices, for educational purposes only. The purpose of these technology resources is to improve learning and teaching through research, collaboration, dissemination of information, and the use of global communication resources.

School district personnel who have been designated by the Superintendent to oversee and coordinate the school district's computer networks/computer systems will monitor computer use, computer networks, and online activity, in any form necessary, to maintain the integrity of the networks, ensure proper use, and to be in compliance with Federal and State laws that regulate Internet safety.

Regulation 2361 applies to the use of district-owned computer networks/computers, as well as the use of privately owned devices, in school.

Definitions

For the purpose of this Policy and Regulation 2361:

- "Computer networks/computers" includes, but is not limited to, computers, computer networks, computer servers, other computer hardware, computer software, and any other computer related equipment, as well as Internet equipment and access. Unless otherwise stated, "computer networks/computers" includes district-owned computer networks/computers as well as privately owned devices.
- "Technology" means hardware or software.
- "Privately owned" means technology hardware and software that is purchased, owned, and maintained by the pupil (or pupil's family) at no expense to the school or school district.
- "Hardware" means any device that can store, access, retrieve, and/or communicate data or information. Hardware may include, but is not limited to, any type of computer device; wireless telephone; electronic reader; personal digital assistant; video broadcasting and/or recording device; or digital camera.
- "Software" means any computer program(s) or related data that provides instruction



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 2 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

for telling a computer or other hardware device what to do and how to do it.

Regulations

Due to the complex association between government agencies, computer networks/computers, and the requirements of Federal and State laws, the end user of the school district's computer networks/computers must adhere to strict regulations. These regulations are provided to assure that all users—including staff, community, pupils, and parent(s)/legal guardian(s) of pupils—are aware of their responsibilities with respect to technology resources.

The school district may modify these regulations at any time. The signatures of the pupil and his/her parent(s) or legal guardian(s) on a district-approved Consent and Waiver Agreement are legally binding and indicate the parties have read these terms and conditions carefully, understand their significance, and agree to abide by the rules and regulations established under Policy 2361, Policy 2363, and Regulation 2361.

Acceptable Use

1. Parent(s) or legal guardian(s) permission is required for a pupil to access the school district's computer networks/computers.
2. Pupils must sign a consent form agreeing to abide by the school district's regulations for using computer networks/computers before they may access the school district's computer networks/computers or use privately owned devices in school.
3. Pupils are responsible for acceptable and appropriate behavior and conduct on computer networks/computers. Communications on computer networks/computers are often public in nature; therefore all policies and regulations governing appropriate behavior and communications apply. Access to computer networks/computers is given to pupils who agree to act in a considerate, appropriate, responsible, and self-aware manner.
4. Pupils may use computer networks/computers to conduct research, complete school assignments, and communicate with others for educational purposes only.
5. Access to the school district's computer networks/computers entails responsibility. Individual users of the district computer networks/computers are responsible for their own behavior and communication over the computer networks/computers. Users are expected to comply with district standards and to honor the agreements they have



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 3 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

signed and the permission they have been granted. Beyond the clarification of such standards, the district is not responsible for the actions of individuals using the computer networks/computers.

6. Computer networks/computer storage areas shall be treated in the same manner as other school storage facilities. School district personnel may review files and communications to maintain system integrity, confirm users are using the system responsibly, and ensure compliance with Federal and State laws that regulate Internet safety. Therefore, no person should expect files stored on district servers to be private.

Prohibited Use

Individuals engaging in the following actions when using the district's computer networks/computers, or when using privately owned devices to access the Internet in school, shall be subject to appropriate discipline and/or legal action:

1. Sending or displaying offensive messages or pictures;
2. Using obscene language and/or accessing material or visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;
3. Using or accessing material or visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;
4. Using or accessing material or visual depictions that are harmful to minors including any pictures, images, graphic image files or other material or visual depictions that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
5. Using or accessing visual images or information that depict, describe, or represent in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct, or that taken as a whole lack serious literary, artistic, political, or scientific value as to minors;
6. Cyberbullying (including, but not limited to, procuring or transmitting any material in violation of cyberbullying, sexual harassment, or hostile workplace laws);
7. Behaving inappropriately online (including, but not limited to, interacting inappropriately with others on social networking sites and in chat rooms, or



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 4 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

posting inappropriate public or private messages);

8. Harassing, insulting, or attacking others;
9. Breaching security (e.g., including, but not limited to, accessing data of others, logging into servers/accounts without authorization);
10. Degrading user account and/or network security and integrity (e.g., including, but not limited to, sharing account information with others, logging in with another user's account, writing down passwords, and/or failing to log off a network computer after use).
11. Damaging computers, computer systems, or computer networks/computers;
12. Intentionally disrupting network traffic or crashing the network (e.g., including, but not limited to, chain letters, junk mail, and spamming);
13. Intentionally disrupting network communication (including, but not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forging routing information for malicious purposes);
14. Introducing malicious programs into the network or server (e.g., including, but not limited to, viruses, worms, Trojan horses, email bombs);
15. Degrading or disrupting equipment or system performance (e.g., including, but not limited to, non-educational web browsing, gaming, file uploading and downloading, and video/music streaming);
16. Engaging in port or security scanning without previously notifying the Board;
17. Executing any form of network monitoring to intercept data intended for another host, unless this activity is a part of the individual's assigned duties;
18. Circumventing user authentication or security of any host, network, or account;
19. Interfering with or denying service to any user other than your host (e.g., a denial of service attack);



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 5 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

20. Using any program/script/command or sending a message of any kind with the intent to interfere with or disable a user's terminal session via any means, locally or via the Internet/intranet/extra net;
21. Violating copyright laws (such as by stealing data or other intellectual property);
22. Using another user's password;
23. Trespassing in, stealing/using, and/or vandalizing another user's folders, work, or files;
24. Trespassing in, stealing/using the property of, and/or vandalizing other resources or entities;
25. Forging email messages or using an account owned by another user;
26. Using the district's computer resources/networks for commercial purposes, financial gain, or fraud (including making fraudulent offers of projects, items, or services from a South Hunterdon account);
27. Providing unauthorized information about, or lists of, students or Board employees to parties outside the Board of Education;
28. Invading the privacy of others (including, but not limited to, using any electronic device to record, by audio or video media, or to photograph students or staff members without the individuals' express, prior permission, or by distributing unauthorized recordings or photographs of such individuals);
29. Posting anonymous messages;
30. Intentionally wasting limited resources;
31. Engaging in other activities that do not advance the educational purposes for which computer networks/computers are provided;
32. Possessing any data which is a violation of this policy; and/or
33. Engaging in any other activity that is disruptive to the school environment or that does not advance the educational purposes for which computer networks/computers are provided.



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 6 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

Privately Owned Devices

The following additional regulations apply only to the use of privately owned devices in school:

1. Any individual who wishes to use a privately owned device to access the Internet in school must first (1) agree in writing to the district's acceptable use policies and regulations relating to technology, and (2) register the device with the staff member designated by the Superintendent to oversee and coordinate the school district's computer networks/computer systems. Users who do not agree to these conditions are not permitted to use privately owned devices to access the Internet in school.
2. Any individual who wishes to use a privately owned device to access the Internet in school must provide current virus (virus definitions not less than two weeks old) and firewall protection for the device(s) from which they will be accessing the Internet.
3. Pupils using privately owned technology to access the Internet during instructional time will access only teacher-approved Internet sites. Any use of privately-owned technology by a pupil shall be in strict accordance with the teaching staff member's specific approval(s) and Board policies and regulations. Any violation will subject the pupil to appropriate discipline and/or grading consequences.
4. Teaching staff members will ensure that the use of privately owned technology in school does not confer any advantage or benefit on pupils who own such technology over pupils who do not. Teaching staff members will not approve the use of privately owned technology if the use would be advantageous or beneficial to the pupil who owns such technology over the pupil who does not own such technology.
5. Pupils who use privately owned devices in school are not permitted to use those devices to access the school district's computer server(s) or network(s). Once approved to use privately owned technology in school (as a result of both executing a consent agreement and getting permission from a staff member), the user will be granted "pass through" access to the Internet only, without the use of any school district hardware or software.



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 7 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

6. Pupils who use privately owned devices in school are not permitted to connect to the internet through other service providers. Personally owned devices may only access the internet via the district's content-filtered wireless network.
7. Personally owned devices are prohibited in locker rooms, restrooms, and nurses offices.

INTERNET SAFETY

Compliance with Children's Internet Protection Act

As a condition for receipt of certain Federal funding, the school district has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter material or visual depictions that are obscene, that may be considered child pornography, and that may be harmful to minors as defined in regulations 2, 3, 4, 5, 6, and 7 under Prohibited Use, above, and in the Children's Internet Protection Act. The school district will certify the schools in the district, including media centers/libraries, are in compliance with the Children's Internet Protection Act and that the district complies with and enforces Policy and Regulation 2361.

Compliance with Neighborhood Children's Internet Protection Act

In keeping with the Neighborhood Children's Internet Protection Act, Policy 2361 and this Regulation establish Internet safety protection policy and procedures that address:

1. Access by minors to inappropriate matter on the Internet and World Wide Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication;
3. Unauthorized access, including "hacking" and other unlawful activities by minors online;
4. Cyberbullying;
5. Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 8 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

6. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and
7. Measures designed to restrict minors' access to materials that are harmful to minors.

Notwithstanding the material or visual depictions defined in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Board shall determine Internet material that is inappropriate for minors.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on Internet safety protection Policy and Regulation 2361. Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed **at the annual public hearing**.

Information Content and Uses of the System

Pupils may not publish on or over the system any information which violates or infringes upon the rights of any other person, or any information which would be abusive, profane, or sexually offensive to a reasonable person, or which, without the approval of the Superintendent of Schools or designated school district personnel, contains any advertising or any solicitation to use goods or services. A pupil cannot use the facilities and capabilities of the system to conduct any business or solicit the performance of any activity that is prohibited by law.

Because the school district provides, through connection to the Internet, access to other computer systems around the world, pupils and their parent(s) or legal guardian(s) should be advised that the Board and school district personnel have no control over content. While most of the content available on the Internet is not offensive, and much of it is a valuable educational resource, some objectionable material exists. Even though the Board provides pupils access to Internet resources through the district's computer networks/computers with installed appropriate technology protection measures in place, parents and pupils must be advised that potential dangers remain and offensive material may be accessed in spite of the technology protection measures taken by the school district.

Pupils and their parent(s) or legal guardian(s) are advised that some systems and Internet sites may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material. The



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 9 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

Board and school district personnel do not condone the use of such materials and do not permit usage of such materials in the school environment. Parent(s) or legal guardian(s) having Internet access available to their children at home should be aware of the existence of such materials and monitor their child's access to the school district system at home. Pupils knowingly bringing materials prohibited by Policy 2363 or Policy and Regulation 2361 into the school environment will be disciplined in accordance with Board policies and regulations, and such activities may result in termination of such pupils' accounts or access on the school district's computer networks and their independent use of computers.

Online Conduct

Any action by a pupil or other user of the school district's computer networks/computers that is determined by school district personnel to constitute an inappropriate use of the district's computer networks/computers or to improperly restrict or inhibit other persons from using and enjoying those resources is strictly prohibited and may result in limitation or termination of an offending person's access and other consequences in compliance with Board policy and regulation. The user specifically agrees not to submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information, or software in violation of any local, State, or Federal law is also prohibited and is a breach of the Consent and Waiver Agreement. Computer networks/computer resources are to be used by the pupil for his/her educational use only; commercial uses are strictly prohibited.

Pupils and their parent(s) or legal guardian(s) specifically agree to indemnify the South Hunterdon Regional school district and school district personnel for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this section by the pupil.

Software Libraries on the Network

Software libraries used on or through the school district's computer networks/computers are provided to pupils as an educational resource. No pupil may install, upload, or download software without the expressed consent of appropriate school district personnel. Any software having the purpose of damaging another person's accounts or information on the school district computer networks/computers (e.g., computer viruses) is specifically prohibited. School district personnel reserve the right to refuse posting of files and to remove files. School district personnel further reserve the right to



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM
2361 / Page 10 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

immediately limit usage or terminate the pupil's access or take other action consistent with the Board's policies and regulations of a pupil who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer networks/computers without authorization. Pupils may download copyrighted material for their own use in accordance with Policy and Regulation 2531, Use of Copyrighted Materials. A pupil may only redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author or authorized source.

Public Posting Areas (Message Boards, Blogs, Etc.)

School district personnel have no control of the content of messages that are posted from systems connected to the Internet around the world. To best utilize system resources, school district personnel will determine message boards, blogs, etc., that are most applicable to the educational needs of the school district and will permit access to these sites through the school district computer network. School district personnel may remove messages that are deemed to be unacceptable or in violation of Board policies and regulations. School district personnel further reserve the right to immediately terminate the access of a pupil who misuses these public posting areas.

Real-time, Interactive, Communication Areas

School district personnel reserve the right to monitor and immediately limit the use of the computer networks/computers or terminate the access of a pupil who misuses real-time conference features (talk/chat/Internet relay chat).

Electronic Mail

The school district may or may not establish pupil email accounts. In the event the district provides email accounts, all messages sent and received on the school district computer networks/computers must have an educational purpose and are subject to review. Messages received by a district-provided email account are retained on the system until deleted by the pupil or for a period of time determined by the district. A canceled account will not retain its emails. Pupils are expected to remove old messages, as needed, at the end of the school year, or in the event a mailbox quota is reached, or school district personnel may remove such messages. School district



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 11 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

personnel may inspect the contents of emails sent by a pupil to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by policy, regulation, or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, State, or Federal officials in any investigation concerning or relating to any email transmitted or any other information on the school district computer networks/computers.

Disk Usage

The district reserves the right to establish maximum storage space a pupil receives on the school district's system. A pupil who exceeds his/her quota of storage space will be advised to delete files to return to compliance with the predetermined amount of storage space. A pupil who remains in noncompliance of the storage space allotment after seven school days of notification may have their files removed from the school district's system.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a pupil identifies a security problem on the computer networks/computers, the pupil must notify the appropriate school district staff member. The pupil should not inform other individuals of a security problem. Passwords provided to pupils by the district for access to the district's computer networks/computers or developed by the pupil for access to an Internet site should not be easily guessable by others or shared with other pupils. Attempts to log in to the system using either another pupil's or person's account may result in termination of the account or access. A pupil should immediately notify the Principal or designee if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any pupil identified as a security risk will have limitations placed on usage of the computer networks/computers or may be terminated as a user and be subject to other disciplinary action.

Vandalism

Vandalism to any district-owned computer networks/computers may result in cancellation of system privileges and other disciplinary measures in compliance with the district's discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other computer networks/computers that are connected to the Internet backbone or of doing intentional



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM

2361 / Page 12 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

Printing

The printing facilities of the computer networks/computers should be used judiciously. Unauthorized printing for other than educational purposes is prohibited.

Staff Internet Sites and the World Wide Web

Designated school district staff may establish Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by the staff members who create them, who shall ensure the content of the site complies with Federal, State, and local laws and regulations as well as Board policies and regulations.

Violations

Violations of the district's Acceptable Use of Computer Networks/Computers and Resources Policy and Regulation or Policy 2363 may result in a loss of access as well as other disciplinary or legal action. Disciplinary action shall be taken as indicated in Policy and/or Regulation 2361 Acceptable Use of Computer Networks/Computers and Resources; Policy 2363; Policy and/or Regulation 5600 Pupil Discipline/Code of Conduct; Policy and/or Regulation 5610 Suspension; and Policy and/or Regulation 5620 Expulsion; as well as possible legal action and reports to the legal authorities and other entities.

Determination of Consequences for Violations

The particular consequences for violations of Policy 2363 or Policy and/or Regulation 2361 shall be determined by the Principal or his/her designee. The Superintendent or his/her designee and the Board shall determine when school expulsion and/or legal action or actions by the authorities is the appropriate course of action.

Individuals violating Policy 2363 or Policy and/or Regulation 2361 shall be subject to the consequences as indicated herein and other appropriate discipline, which includes but is not limited to:

1. Use of computer networks/computers only under direct supervision;
2. Suspension of network privileges;



REGULATION

SOUTH HUNTERDON REGIONAL BOARD OF EDUCATION

PROGRAM
2361 / Page 13 of 13

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. Legal action and prosecution by the authorities.

Issued: 29 April 2004
Revised: 21 February 2013

