R 2361 ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS/PERSONAL ELECTRONIC DEVICES (PEDS) AND RESOURCES

The school district provides computer equipment, computer services, and Internet access to its pupils and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources.

For the purpose of this Policy and Regulation, "computer networks/computers and PEDs" includes but is not limited to, the school district's computer networks, computer servers computers, other computer hardware and software, Internet equipment and access, and any other computer related equipment, including telephone systems, video surveillance system, and peripherals (document cameras, projectors, etc.) Additionally, this Policy and Regulation includes Personal Electronic Devices (PEDs) as referenced in Policy 2363.

For the purpose of this Policy and Regulation, "school district personnel" shall be the person(s) designated by the Superintendent of Schools to oversee and coordinate the school district's computer networks/computer systems and PEDs. School district personnel will monitor 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.

Due to the complex association between government agencies and computer networks/computers and PEDs and the requirements of Federal and State laws, the end user of computer networks/computers and PEDs must adhere to strict regulations. Regulations are provided to assure staff, community, pupils**,** and parent(s) or legal guardian(s) of pupils are aware of their responsibilities. 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 the terms and conditions carefully, understand their significance, and agree to abide by the rules and regulations established under Policy and Regulation 2361.

Pupils are responsible for acceptable and appropriate behavior and conduct on school district computer networks/computers and PEDs. Communications on the computer networks/computers and PEDs are often public in nature and policies and regulations governing appropriate behavior and communications apply. The school district's networks, Internet access, and computers are provided for pupils to conduct research**,** complete school assignments, and communicate with others. Access to computer networks/computers and PEDs is given to pupils who agree to act in a considerate**,** appropriate, and responsible manner. Parent(s) or legal guardian(s) permission is required for a pupil to access the school district's computer networks/computers and PEDs. Access entails responsibility and individual users of the district computer networks/computers and PEDs are responsible for their behavior and communications over the computer

networks/computers and PEDs. It is presumed users will comply with district standards and will honor the agreements they have signed and the permission they have been granted. Beyond the clarification of such standards, the district is not responsible for the actions of individuals utilizing the computer networks/computers and PEDs who violate the policies and regulations of the Board.

Computer networks/computer and PEDs 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 will be private or confidential.

The following prohibited behavior and/or conduct using the school district's networks/computers and PEDs, includes-but is not limited to the following:

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. Depicting, describing, or representing in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

6. Cyberbullying (for example – see #8);

7. Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;

8. Harassing, insulting or attacking others through medias such as social networking, texts, blogs, etc.

9. Damaging computers, computer systems or computer networks/computers and PEDs;

10. Violating copyright laws;

11. Using another's username, password, or pin numbers;

12. Attempting to "hack" the district network by improperly obtaining staff member passwords, including, but not limited to, observation and/or installing key stroke recording programs.

13. Trespassing in another's folders, work or files;

14. Intentionally wasting limited resources;

15. Employing the network/computers for commercial purposes; and/or

16. Engaging in other activities that do not advance the educational purposes for which computer network/computers are provided.

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, child pornography and harmful to minors as defined in 2, 3, 4, 5, 6, and 7 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 the district complies with and enforces Policy and Regulation 2361.

Compliance with Neighborhood Children's Internet Protection Act

Policy 2361 and this Regulation establish an Internet safety protection policy and procedures to 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 communications;

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;
6. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and
7. Measures designed to restrict minors access to materials 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 the Internet safety protection policy - Policy and Regulation 2361. Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

PRIVACY

Compliance with Children's Online Privacy and Protection Act (COPPA) Notice

Policy 2361 and this Regulation establish an Internet safety protection policy and procedures for children under the age of 13 to address:

1. Posting a clear and comprehensive online privacy policy describing website and app information practices for personal information collected online from children;

2. Providing direct notice to parents and obtaining verifiable parental consent, with limited exceptions, before collecting personal information online from children;

3. Giving parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);

4. Providing parents access to their child's personal information to review and/or have the information deleted;

5. Giving parents the opportunity to prevent further use or online collection of a child's personal information;

6. Maintaining the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and

7. Retaining personal information collected online from a child only as long as necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.

COPPA permits school districts, such as ours, to provide consent to the collection of personal information strictly for educational purposes on behalf of all of its students. This eliminates the need for parents to provide direct consent to each digital service the school utilizes in your child's instruction.

The District will maintain a listing of websites and apps utilized by our schools on our district website (www.ridgewood.k12.nj.us). Websites and apps may not be used by all grades or by all levels. While no vendor will offer a guarantee of complete and perpetual security, the Terms of Service and Privacy Policy statements for those vendors listed have been reviewed (as are updates to change them) to verify that appropriate security and privacy measures are in place to protect those using the service. Please contact the Manager of Information Technology or the Superintendent of Schools for more information.

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 which 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 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 and PEDs with installed appropriate technology protection measures, parents and pupils must be advised that potential dangers remain and offensive material may be accessed notwithstanding the technology protection measures taken by the school district.

Pupils and their parent(s) or legal guardian(s) are advised some systems and Internet sites may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material. The 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. Pupils knowingly bringing materials prohibited by 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 pupil's accounts or access on the school district's computer network**s** and their independent use of computers.

On-line Conduct

Any action by a pupil or other user of the school district's computer networks/computers and PEDs 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 on 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.

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

Computer networks/computer resources and PEDs are to be used by the pupil for his/her educational use only; commercial uses are strictly prohibited.

Software Libraries on the Network

Software libraries on or through the school district's networks 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 further reserve the rights to refuse posting of files and to remove files. School district personnel further reserve the right to 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 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.)

Messages are posted from systems connected to the Internet around the world and school district personnel have no control of the content of messages posted from these other systems. 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 networks. 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

Electronic mail ("e-mail") is an electronic message sent by or to a person in correspondence with another person having Internet mail access. 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 within fifteen days or school district personnel may remove such messages. School district personnel may inspect the contents of e-mail**s** 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 the 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 e-mail 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/computer, 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 and PEDs 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 or pin number is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their accounts. Any pupil identified as a security risk will have limitations placed on usage of the computer networks/computers and PEDs or may be terminated as a user and be subject to other disciplinary action.

Vandalism

Vandalism to any school district owned computer networks/computers and PEDs 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 network**s**/computers and PEDs that are connected to the Internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses. In the event vandalism results in a financial loss to the district, restitution by the offender may be required.

Printing

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

Internet Sites and the World Wide Web

Designated school district personnel may establish an Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by the designated school district personnel 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 Acceptable Use of Computer Network**s**/Computers and PEDs and Resources Policy and Regulation 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/PEDs and Resources, 5600 Pupil Discipline/Code of Conduct, 5610 Suspension and 5620 Expulsion as well as possible legal action and reports to the legal authorities and entities.

Determination of Consequences for Violations

The particular consequences for violations of this Policy shall be determined by the Principal or designee. The Superintendent or 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 this Policy shall be subject to the consequences as indicated in Board Policy and Regulation 2361 and other appropriate discipline, which includes but are not limited to:

1. Use of computer networks/computers and PEDs only under direct supervision;

2. Suspension of network privileges;

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: 7 December 2009
Revised: 18 June 2012
Revised: 24 September 2012
Revised: 6 March 2017