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

The Board of Education recognizes as new technologies shift the manner in which information is accessed, communicated and transferred; these changes will alter the nature of teaching and learning. Access to technology will allow students to explore databases, libraries, Internet sites, and bulletin boards while exchanging information with individuals throughout the world. The Board supports access by students to these information sources but reserves the right to limit in-school use to materials appropriate for educational purposes. The Board directs the Superintendent to affect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes technology allows students access to information sources that have not been pre-screened by educators using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer networks/computers and PEDs and declares unethical, unacceptable or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The Board provides access to computer networks/computers and PEDs for educational purposes only. The Board retains the right to restrict or terminate student access to computer networks/computers and PEDs at any time, for any reason. School district personnel will monitor networks and online activity to maintain the integrity of the networks**,** ensure their proper use**,** and ensure compliance with Federal and State laws that regulate Internet safety.

Standards for Use of Computer Networks/Computers and PEDs

Any individual engaging in the following actions when using computer networks/computers and PEDs shall be subject to discipline or legal action:

A. Using the computer network(s)/computers and PEDs for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities that violate federal, state, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the networks. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.

B. Using the computer network(s)/computers and PEDs to violate copyrights, institutional or third party copyrights, license agreements or other contracts.

C. Using the computer network(s)/computers and PEDs in a manner that:

1. Intentionally disrupts network traffic or crashes the network;

2. Degrades or disrupts equipment or system performance;

3. Uses the computing resources of the school district for commercial purposes, financial gain, or fraud;

4. Steals data or other intellectual property;

5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another person;

6. Gains or seeks unauthorized access to resources or entities;

7. Forges electronic mail messages or uses an account owned by others;

8. Invades privacy of others;

9. Posts anonymous messages;

10. Possesses any data which is a violation of this Policy; and/or

11. Engages in other activities that do not advance the educational purposes for which computer networks/computers and PEDs are provided.

Internet Safety/Protection

As a condition for receipt of certain Federal funding, the school district shall be in compliance with the Children's Internet Protection Act**,** the Neighborhood Children's Internet Protection Act, and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries. The technology protection must block and/or filter material and visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors

including any pictures, images, graphic image file or other material or visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents 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.

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

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

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent of Schools or designee will develop and ensure education is provided to every student regarding appropriate online behavior, including students interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

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 policy – Policy and Regulation 2361. Any changes in Policy and Regulation since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

The school district will certify on an annual basis, that the schools, including media centers/libraries in the district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

Consent Requirement

No student shall be allowed to use the school district's computer networks/computers Internet and any other third party online services employed by the district unless consent is given for the student by his/her parent(s) or legal guardian(s).

In order to meet our educational goals, Ridgewood Public Schools may utilize third party websites and online services, (such as sites and apps for curriculum, graphic design and foreign language), for our students. These services are used to assist with curricular and other education specific needs both inside and outside of the classroom. The school, when possible and appropriate, will utilize the education specific versions and also restrict the student information shared with these services to the minimum required for account creation.

COPPA

Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998 with amendments in 2012. The primary purpose of COPPA is to place parents in control over the information gathered about their children by online apps. The Rule applies to commercial websites/apps that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using or disclosing personal information from children under 13.

For students under the age of 13, 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.

Parents wishing to deny access to these educational tools, must do so in writing to the principal indicating their child should be denied access to these tools. It should be noted that because RPS provides your child a relevant education through integrated technology, denying access to these educational tools will prove problematic for any classes utilizing Chromebooks for instructional purposes. For more information on COPPA, please visit https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online.

G Suite For Education (Formerly Google Apps for Education or GAFE)

Ridgewood Public School District uses G Suite for Education and other digital resources to facilitate learning through research, communication, collaboration and creativity. G Suite is a collection of free online applications, such as a word processor, spreadsheet, a presentation program, as well as online file storage.

G Suite is provided by Google specifically for educational institutions. As such, Google does not collect or use student data in G Suite for advertising or ad creation. In addition, all advertisements are turned off in G Suite services. So if your child is logged into his or her G Suite account, he or she will not see ads when using Google Search.

All students are given a District-owned Google account. These accounts are managed by the District and not by Google. Your child's Google account allows access to Google's online applications and file storage (Google Drive) from any web browser. Students are expected to adhere to the rules and regulations for email use as outlined in the signed District Acceptable Use of Networks/Computers Policy (AUP).

These District-issued accounts are only for educational purposes and are NOT meant for registering to online social networks (i.e. Instagram, Facebook), or subscribing to internet/public community sites that are not educational in nature, unless otherwise directed by their teacher.

Access to and use of G SUITE at schools is considered a privilege. The District maintains the right to immediately withdraw the access and use of G SUITE when there is reason to believe that violations of law or District policies have occurred. The District also reserves the right to monitor G SUITE and any online services used by students for improper use.

Violations

Individuals violating this Policy shall be subject to the consequences as indicated in Regulation 2361 and other appropriate discipline, which includes but are not limited to:

1. Use of the network 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.

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