

4321 ACCEPTABLE USE OF COMPUTER NETWORK(S)/COMPUTERS/PERSONAL
ELECTRONIC DEVICES (PEDS) AND RESOURCES BY SUPPORT STAFF MEMBERS

The Board 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 support staff members to explore databases, libraries, Internet sites, and bulletin boards while exchanging information with individuals throughout the world. The Board supports access by support staff members 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 effect training of support staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes that technology allows support staff members access to information sources that have not been pre-screened using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer network(s)/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 network(s)/computers and PEDs for administrative and educational purposes only. The Board retains the right to restrict or terminate support staff members' access to the computer network(s)/computers and PEDs at any time, for any reason. The Board retains the right to have the Superintendent or designee 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 Network(s)/Computers and PEDs

Any individual engaging in the following actions when using computer network(s)/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 which 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.



POLICY

RIDGEWOOD BOARD OF EDUCATION

SUPPORT STAFF MEMBERS

4321/page 2 of 4

Acceptable Use of Computer Network(s)/Computers/
Personal Electronic Devices (PEDS) and
Resources by Support Staff Members

- 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 user;
 - 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 network(s)/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 pupil regarding appropriate online behavior, including pupils 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.



POLICY

RIDGEWOOD BOARD OF EDUCATION

SUPPORT STAFF MEMBERS

4321/page 4 of 4

Acceptable Use of Computer Network(s)/Computers/
Personal Electronic Devices (PEDS) and
Resources by Support Staff Members

Consent Requirement

No pupil shall be allowed to use the school districts' computer networks/computers and PEDs and the Internet unless they have filed with the office a consent form signed by the pupil and his/her parent(s) or legal guardian(s).

Violations

Individuals violating this policy shall be subject to appropriate disciplinary actions as defined by Policy No. 4150, Discipline which includes but are not limited to:

1. Use of the network(s)/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;
7. Dismissal;
8. Legal action and prosecution by the authorities; and/or
9. Any appropriate action that may be deemed necessary as determined by the Superintendent and approved by the Board of Education.

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 March 2013

