2361 ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES (M)

M

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

The Board also recognizes technology allows pupils 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 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 for educational purposes only. The Board retains the right to restrict or terminate pupil access to computer networks/computers 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

Any individual engaging in the following actions when using computer networks/computers or a non-Board of Education supplied device shall be subject to discipline or legal action:

A. Using the computer networks/computers 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 networks/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.

C. Using the computer networks or a non-Board of Education supplied device in a manner that:

1. Intentionally disrupts network traffic or crashes the network--included, but not limited to chain letters, junk mail and spamming;

2. Degrades or disrupts equipment or system performance;

3. Uses the computing resources of our 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;

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

12. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.);

13. Using a Bernards Township Board of Education computing asset to procure or transmit material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction;

14. Making fraudulent offers of projects, items, or services originating from any Bernards Township Board of Education account;

15. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which you are not an intended recipient or logging into a server or account that you are not expressly authorized to access, unless these duties are within the scope of regular duties. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;

16. Port scanning or security scanning, unless you previously notify Bernards Township Board of Education;

17. Executing any form of network monitoring that will intercept data not intended for your host, unless this activity is a part of your normal 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 (for example, a denial of service attack);

20. Using any program/script/command, or sending messages 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/extranet;

21. Providing unauthorized information about, or lists of, Bernards Township Board of Education employees to parties outside Bernards Township Board of Education;

22. Use that is disruptive to the school environment;

23. For security and network maintenance purposes, authorized individuals within Bernards Township Board of Education may monitor equipment, systems and network traffic at any time, per the Audit Policy; and/or

24. Bernards Township Board of Education reserves the right to audit networks and systems on a periodic basis to ensure compliance with the policy.

Standards for Use of Non-Board of Education Issued Devices (BYOT)

Any individual using non-Board of Education issued devices accepts that such usage is only permitted by agreeing to all district policies and procedures relating to technology. Users who do not agree to these conditions are not permitted to use non-Board of Education devices on school grounds during school hours. **A non-Board of Education issued device is any device not owned by the Board of Education. Examples of a non-Board of Education issued device includes phones, smart phones, smart watches, tablets, laptops, smart glasses, etc. that are owned by students, staff or parents.**

User's Obligations: All users agree to provide virus and firewall protection for any device(s), from which users will be accessing the computer network. Virus protection software must be updated with virus definitions not less than two weeks old.

User's Assumption of All Risks of Use: Users agree to and hereby assume all risks (including, but not limited to, the risks of damage caused by hackers, worms, Trojans or viruses) arising from, connected to or resulting from usage of this computer network or non-Board of Education supplied devices.

User's Acknowledgments: All users acknowledge: 1) the use of the Board of Education computer network may not be uninterrupted or error-free; 2) use of the Board of Education computer network may expose you or your device(s) to risks such as hackers, worms, Trojans or viruses; 3) although the Bernards Township Board of Education makes great effort to keep the computer network safe and secure for users, Bernards Township Board of Education does not guarantee the security of this computer network; 4) unauthorized third parties may access your device(s) or files or otherwise monitor your use of this computer network; 5) the Bernards Township Board of Education's ability to provide this access the computer network without charge is based on the disclaimers and limitations of liability provided in the "Indemnification" and "Limitation of Liability" paragraphs below. 6) The district does not provide specific network access for non-Board of Education supplied devices nor does it offer technical support for their use.

User's Restrictions: Schools shall be guided by the following usage restrictions for students who bring non-Board of Education issued devices to school.

KG-5: All devices shall remain off and away stored with students personal belongings. Students are not to use any privately-owned devices during the regular instructional day in any setting.

6-8: All devices shall remain off and stored in the student's locker. Students may use the devices during instructional periods only if their teacher provides explicit

permission to do so. Students are not permitted to use devices in the hallway or during non-instructional periods such as lunch or study periods.

9-12: During instructional periods, all devices must be off and stored away in locations designated by the classroom teacher. Storage locations may include "pho-tels," bins, shelves or other location set by the teacher; students may not store their device on their person during instructional periods Students may not have devices on their person during instructional periods unless given explicit permission from the teacher to retrieve the device from the designated storage location to use for instructional purposes. Students may use personal devices in non-instructional settings such as halls, the cafeteria, or study halls.

Limitation of Liability: Under no circumstances will the Bernards Township Board of Education or any of their administrators, officers, directors, employees, agents or affiliates be liable for any legal damages (whether based on tort, breach of contract or equitable theories) based on any claim of the user, or any of the user's heirs, assignees, appointees or successors-in-interest, and arising out of or as a result of the user's use of the computer network or non-Board of Education supplied devices.

Indemnification: All users agree to indemnify and hold harmless the Bernards Township Board of Education and each of their suppliers, licensors, officers, directors, employees, agents or affiliates from any claim, lawsuit, liability, loss, damage, cost, expense or attorney's fee arising out of or relating to any actions initiated or caused by users while using this computer network or non-Board of Education supplied devices.

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 2361 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.

The Board of Education is not capable of filtering the content for pupils using non-Board of Education supplied devices that are capable of accessing the internet via non district network access, such as cellular phone networks. Parents/guardians assume all responsibility for unfiltered pupil access to the internet via non-Board of Education internet connections such as cellular phone networks, Wi-Max, etc.

Consent Requirement

No pupil shall be allowed to use Board of Education computers and network, or non-Board of Education supplied devices unless they shall have filed with the respective school office a consent form signed by the pupil and his/her parent(s) or guardian(s).

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 26 August 2013