Policy

ACCEPTABLE USE OF TECHNOLOGY AND RESOURCES

The Saddle River Board of Education recognizes that as telecommunications and other new technologies shift the manner in which information is accessed, communicated and transferred that those changes will alter the nature of teaching and learning. Access to telecommunications will allow pupils, parents, faculty, administration and board members, to explore databases, libraries, Internet sites, bulletin boards and the like while exchanging information with individuals throughout the world. The board supports access by members of the Wandell School community to information sources but reserves the right to limit in-school use to materials appropriate to educational purposes. The board delegates to the superintendent the right to restrict or terminate access to the computer network/computers at any time, for any reason. The board retains the right to have district personnel monitor network activity, in any form necessary, to maintain the integrity of the network and insure its proper use.

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 district utilizes filtering software on all Internet stations to filter and block offensive sites. However, it is impossible to control all searching of materials. Users must be aware of their responsibilities and the consequences that will occur if the access is misused.

E-mail messages shall pertain to education and/or legitimate district business. Because all computer hardware and software belong to the board, the board retains the right to access e-mail and other information stored on its system as it believes necessary. Thus confidentiality of e-mail communication cannot be assured. Staff members shall not reveal their passwords to others in the network or to anyone outside of it. If anyone has reason to believe that a password has been lost or stolen or that e-mail has been accessed by someone without authorization, he/she shall contact superintendent/principal immediately before using the district's equipment or Internet. All staff using the district computers and other electronic devices and the district network must sign this Acceptable Use Policy.

The board recognizes that telecommunications will allow 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.

Standards for Use of Computer networks

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

A. Using the computer network(s)/computers for illegal, inappropriate or obscene purposes, or in support of such activities is prohibited. "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 network. 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 to violate copyrights, institutional or third party copyrights, license agreements or other contracts is prohibited.

C. Using the computer network(s) in a manner that:

    1. Intentionally disrupts network traffic or crashes the network;

ACCEPTABLE USE OF TECHNOLOGY AND RESOURCES (continued)

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

Violations

A. Individuals violating this policy shall be subject to the consequences and other appropriate discipline which includes but is not limited to:

1. Required supervision of network use under direct supervision;
2. Suspension of network privileges:
3. Revocation of network privileges:
4. Suspension of computer privileges:
5. Revocation of computer privileges;
6. Legal action and prosecution by the authorities.

Software Copyright

All employees shall strictly adhere to the copyright laws of the United States. No software shall be copied and/or distributed except in accordance with these laws. All software placed on media workstations or any network for which there is public access shall be copy protected.

Computer Laboratories

The board may provide computer laboratories where clusters of computers and computer peripherals are available. When computer laboratories are provided, they shall be accessible to all teachers and pupils who have a defined educational need for computing facilities.

Broadcast Rights and Copyrights

The board specifically retains the broadcast rights and copyrights to all materials created by employees of the board as part of their responsibilities to the board. Any financial remuneration for the use of such materials shall be retained by the board and specifically dedicated to enhance technology used as part of the educational program.

Computer Security

The superintendent shall develop security procedures to include, but not be limited to, the following areas:

A. Physical Security of Equipment

All computer equipment shall be maintained in a secure manner appropriate to its

B. Data Security

1. Back-up procedures for system files, libraries, and data shall be practiced in a timely fashion;
2. Disaster recovery plans shall be kept up-to-date at all times;
3. Password protection shall be in place and updated periodically.

ACCEPTABLE USE OF TECHNOLOGY AND RESOURCES (continued)

C. Resource security shall be in place to prevent unauthorized access to system files, libraries and data.

Employee Training

All new employees having access to computers and information systems as part of their job responsibilities will be trained in the proper security procedures outlined above. All employees having access to computers and information systems as part of their job responsibilities will be kept up-to-date on current security procedures for equipment and data.

Transaction Audit Trail

Appropriate procedures will be maintained in order to monitor system activity and users as necessary.

Use of Facsimile (FAX Machines)

Fax machines provide a useful means of communicating and shall be subject to the same rules that apply to the use of telephones. All incoming faxes shall be considered confidential mail. No disclosure of the contents of any fax shall be made except to the individual for whom the fax is intended. Any individual violating this confidentiality shall be subject to discipline as provided by the policies and regulations of the board.

Adopted:	December 2008
NJSBA Review/Update:	April 2014
Readopted:	December 2014

Key Words

Acceptable Use, E-mail, Internet, Technology, Website, World Wide Web

Legal References:

N.J.S.A. 2A:38A-1 et seq.	Computer System
N.J.S.A. 2C:20-25	Computer Related Theft
N.J.S.A. 18A:7A-10	NJQSAC
N.J.S.A. 18A:36-35	School Internet websites; disclosure of certain student information prohibited
N.J.S.A. 18A:36-39	Notification by school to certain persons using certain electronic devices; fine
N.J.A.C. 6A:30-1.1et seq.	Evaluation of the Performance of School Districts

17 U.S.C. 101 - United States Copyright Law

47 U.S.C. 254(h) - Children's Internet Protection Act

Possible Cross References:

*2224	Nondiscrimination/affirmative action
*3570	District records
*4111.1	Nondiscrimination/affirmative action
4119.2/4219.1	Harassment, intimidation and bullying
*4119.21	Conflict of interest
*4119.22	Conduct and dress
*4119.23	Employee substance abuse
*4119.26/4219.26	Electronic communication
*4131/4131.1	Staff development, inservice education, visitation, conferences
*4211.1	Nondiscrimination/affirmative action
*4219.21	Conflict of interest
*4219.22	Conduct and dress
*4219.23	Employee substance abuse
*4231/4231.1	Staff development, inservice education, visitation, conferences
*5125	Student records

ACCEPTABLE USE OF TECHNOLOGY AND RESOURCES (continued)

*5131	Conduct and discipline
*5131.1	Harassment, intimidation and bullying
*6121	Nondiscrimination/affirmative action
*6142.10	Internet safety and technology
*6144	Controversial issues
*6173	Home instruction

*Indicates policy is included in the Critical Policy Reference Manual.