POLICY

FRANKLIN TOWNSHIP
BOARD OF EDUCATION

PROGRAM
2361/page 1 of 5
Acceptable Use of Computer Networks/
Computers and Resources

2361 ACCEPTABLE USE OF COMPUTER NETWORKS/
COMPUTERS 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 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 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 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 student 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
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 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 purpose for which computer networks/computers 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 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.

Consent Requirement

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

Security of Administrative Computers

Administrative computing on behalf of the Franklin Township Board of Education represents a very valuable and expensive resource and incurs considerable potential liability to the district. In responsible recognition of these considerations, the administration shall, under the direction of the Superintendent, develop security procedures to ensure that:
1. All administrative computer equipment is maintained in a secure manner;

2. Data security is maintained by means of the following procedures:
   a. Back-up procedures for system files, libraries, and data shall be practiced in a timely fashion.
   b. Disaster recovery plans shall be kept up-to-date at all times.
   c. Password protection shall be in place and up-dated periodically.
   d. Resource security shall be in place to prevent unauthorized access to system files, libraries, and data.

3. Employee training that provides that:
   a. All new employees having, as part of their job responsibilities, access to computers information systems will be trained in the proper security procedures outlined above;
   b. All employees having, as part of their job responsibilities, access to computers and all new employees having, as part of their job responsibilities, access to information systems, will be kept up-to-date on current security procedures for equipment and data; and
   c. A transaction audit trail is available through implementation of appropriate procedures to monitor system activity and users, as necessary.

The Superintendent shall designate a Computer Security Officer to monitor system security procedures and to recommend changes as necessary.

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: