2361 ACCEPTABLE USE FOR COMPUTER NETWORK, COMPUTERS, PERSONAL ELECTRONIC DEVICES (PEDs) AND TECHNOLOGY RESOURCES

The Westfield Board of Education endorses the use of the District's computer network, computers, personal electronic devices (PEDs) and technology resources for administrative and educational purposes to enhance instruction, learning, and the day to day operation of the school District. The Board recognizes that technology allows pupils access to information sources that may not have been pre-screened by educators. However, the Board expects that all educators will be conscientious in supporting pupils' learning through access to technology as well as teaching pupils ways to remain safe while utilizing it. The Board supports access by pupils to these information sources but reserves the right to limit in-school or home use of District equipment to materials and processes appropriate for educational purposes.

Access to the District computer network, computers, PEDs, and technology resources is limited to members of the school community involved with school-related functions. That community includes District personnel, pupils and non-District authorized users. Non-District authorized users are community members, parents and guests who have been authorized by school administrators to have network access to assist pupils and teachers and/or to find public information about the District.

For the purpose of this Policy and Regulation, "computer networks, computers, PEDs, and technology resources" includes, but is not limited to, all District owned computer hardware and software, District owned wired and wireless networks, mobile broadband service when accessed on District property, and any other computer related equipment.

For the purpose of this Policy and Regulation, "PEDs" includes those devices owned by individual District personnel, pupils and non-District authorized users and those devices owned by the District and used in the classroom. This definition does not differentiate between accessing the internet through the District owned and operated wireless networks, or through a third party mobile broadband service when accessed on District property.

For the purpose of this Policy and Regulation, "school District personnel" shall be the person(s) designated by the Superintendent to oversee and coordinate the school computer networks/computer systems.

The Board of Education cannot guarantee that the functions or services provided by or through the computer network, computers and technology resources will be error-free. The Board is not responsible for damage users may suffer, including, but not limited to, loss of data, files, or service. The Board will not be responsible for financial obligations due to unauthorized use of the network, computers or technology resources or for violation of the Acceptable Use Policy (AUP) regulations. Due to the fact that the network is connected to the internet, the Board of Education is not responsible for the accuracy or quality of information obtained through or stored on the network or computers. The Board also recognizes technology allow**s** pupils access to information sources that have not been pre-screened by educators using Board approved standards. The Board directs District personnel to provide filtering software and supervision of pupils accessing the internet.

The Board defines its public school setting as a limited public forum; as such, utilization of the network, computers, and technology resources must be directly related to the administrative and educational goals and objectives of the District. The Westfield Public Schools are a public entity and therefore, all records, (except those specifically excluded by law) including electronic data and files, are subject to the NJ Public Records Act and open to public inspection. All files, emails, attachments, and data are not private.

In addition, the use of information technology is a privilege, not a right. Inappropriate use, including any violation of the conditions and rules set forth in this policy and other District policies may result in revocation of such privileges. The Superintendent or designee, under this policy, has the authority to determine appropriate use and may deny, revoke, or suspend any user access at any time based upon a determination of inappropriate use.

District personnel and pupils violating this policy shall be subject to the consequences as indicated in Regulation 2361 and/or the Conduct Discipline/Code of Conduct policy (5500). Non-District authorized users violating this policy shall have their authorization and access revoked.

Standards for Use of Computer Networks

The Board directs the Superintendent to establish standards for the use of the District network and a description of consequences for misuse.

The Board therefore adopts the following standards of conduct for the use of computer networks, computers, PEDs, and technology resources 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.

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; 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 Superintendent or designee shall determine other internet material that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent 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 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

The Board directs the Superintendent to establish a procedure to obtain parent's/guardian's consent/non-consent for their child's use of the computer networks, computers, PEDs technology

resources and internet. Guidelines and expectations for the use of PEDs are outlined in student handbooks. No pupil shall be allowed to use the school Districts' computer networks, computers, PEDs or the internet unless they have filed with the school office a consent form signed by the pupil and his/her parent(s) or legal guardian(s).

Violations

The Board directs the Superintendent to provide rules and regulations governing issues pertaining to the Acceptable Use Policy (AUP) of the District's computer network, computers, PEDs, and technology resources. The Chief Technology Officer, Building Administrators, and District supervisors in accordance with their particular job-related responsibilities, will be expected to support and enforce the AUP and its regulations, provide professional development for administrators, faculty and staff, establish adequate supervision of pupils using the network and resources, and maintain license agreements with vendors.

The Board directs the Superintendent to identify consequences for individuals who violate this policy.

The Board requires that all members of the Westfield educational community abide by the Acceptable Use Policy and Regulations to ensure the effective and appropriate utilization and integration of technology in the educational programs and administrative processes.

The Board will review this Policy and Regulation annually. Any changes to the policy will be discussed at a public meeting to allow for community input.

N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act.
Federal Communications Commission: Neighborhood Children's Internet Protection Act

Related Policies:
2432 School Sponsored Publication in All Media
5500 Code of Conduct
5512 Harassment, Intimidation and Bullying
5610 Suspension
5620 Expulsion
9120 Public Information Program

Approved: December 7, 1999
Revised: June 12, 2012
Revised: August 26, 2014
Reviewed: November 10, 2015
Revised: May 10, 2016
Reviewed: May 26, 2020

R 2361 ACCEPTABLE USE OF COMPUTER NETWORKS, COMPUTERS, PERSONAL ELECTRONIC DEVICES (PEDs) AND TECHNOLOGY RESOURCES

The Westfield Public School's Acceptable Use Regulations will govern the use of the District's computer network, computers, personal electronic devices (PEDs) and technological resources by District personnel, pupils, and non-District authorized users. Non-District authorized users are community members, parents and guests who have been authorized by school administrators to have network access to assist pupils and teachers or to find public information about the District. The purpose of providing these resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources.

School District personnel will monitor networks and online activity, in any form necessary, to maintain the integrity of the networks, ensure proper use, and to be in compliance with Federal and State laws that regulate internet safety.

Due to the complex association between government agencies and computer networks/computers and the requirements of Federal and State laws, the end user of the school District's computer networks/computers must adhere to strict regulations. Regulations are provided to assure staff, community, pupils, and parent(s) or legal guardian(s) of pupils are aware of their responsibilities. The school District may modify these regulations at any time.

All District personnel, pupils in grades 3-12, parents/guardians of pupils in grades K-12, and non-District authorized users connecting to the computer network using District provided devices are required to sign an Acceptable Use of Computers, Personal Electronic Devices (PEDs) and Internet Agreement form to indicate that they have read, understand, and agree to abide by this Policy and Regulations. Pupils in grades K-2 will be guided in an age appropriate manner by their teachers and/or parents as to Acceptable Use of Computers, Personal Electronic Devices (PEDs) and internet access.

The signatures of the pupil and his/her parent(s) or legal guardian(s) on a District-approved form entitled, Acceptable Use for Computer Network, Computers, Personal Electronic Devices (PEDs) and Technology Resources are legally binding and indicate the parties have read the terms and conditions carefully, understand their significance, and agree to abide by the rules and regulations established under Policy and Regulation 2361.

District personnel, pupils, and non-District authorized users are responsible for acceptable and appropriate behavior and conduct on District computer networks, computers, PEDs and technology resources. Communications on the computer networks, computers, PEDs and technology resources are often public in nature and policies and regulations governing appropriate behavior and communications apply. The school District's computer networks, computers, PEDs and technology resources are provided for pupils to conduct research, complete school assignments, and communicate with others. Access to computer networks, computers, PEDs and technology resources is given to District personnel, pupils, and non-District authorized users who agree to act in a considerate, appropriate, and responsible manner. Parent(s) or legal guardian(s) permission is required for a pupil to access the school District's computer networks, computers, PEDs and technology resources. It is presumed users will comply with District standards and will honor the agreements they have signed and the permission they have been granted. Beyond the clarification of such standards, the District is not responsible for the actions of individuals utilizing the computer networks, computers, PEDs and technology resources who violate the policies and regulations of the Board.

Computer networks/computer storage areas shall be treated in the same manner as other school storage facilities. School District personnel may review files and communications to maintain system integrity, confirm users are using the system responsibly, and ensure compliance with Federal and State laws that regulate internet safety. Therefore, no person should expect files stored on District servers will be private or confidential.

Because the school District provides, through connection to the internet, access to other computer systems around the world, pupils and their parent(s) or legal guardian(s) should be advised the Board and school District personnel do not have total control over content. While most of the content available on the internet is not offensive and much of it is a valuable educational resource, some objectionable material exists. Even though the Board provides District personnel, pupils, and non-District authorized users access to internet resources through the District's computer networks, computers, PEDs and technology resources with installed appropriate technology protection measures, parents and pupils must be advised potential dangers remain and offensive material may be accessed notwithstanding the technology protection measures taken by the school District.

Pupils and their parent(s) or legal guardian(s) are advised some systems and internet sites may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material. The Board and school District personnel do not condone the use of such materials and do not permit usage of such materials in the school environment. Parent(s) or legal guardian(s) having internet access available to their children at home should be aware of the existence of such materials and monitor their child's access to the school District system at home. Pupils knowingly bringing materials prohibited by

Policy and Regulation 2361 into the school environment will be disciplined in accordance with Board policies and regulations and such activities may result in termination of such pupils' accounts or access on the District's computer networks and their independent use of computers.

Prohibited behavior and/or conduct using the District's computer networks, computers, PEDs and technology resources includes, but is not limited to:

1. sending or displaying offensive messages or pictures;

2. using the District's computer networks, computers, PEDs and technology resources 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 as indicated in the Conduct-Discipline Code of Conduct policy (5500). Inappropriate activities are defined as those that violate the intended use of the network**s**. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles as set forth in Section 1460 of Title 18, U.S.C.

3. using or accessing material or visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;

4. using or accessing material or visual depictions that are harmful to minors including any pictures, images, graphic image files or other material or visual depictions that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

5. depicting, describing, or representing 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;

6. cyberbullying;

7. inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;

8. harassing, insulting, or attacking others;

9. degrading or disrupting computers, computer systems, or computer networks/computers equipment or system performance;

10. violating copyright laws;

11. gaining or seeking unauthorized access to the files of others or vandalizing the data of another person;

12. trespassing in another's folders, work or files;

13. intentionally wasting limited resources;

14. employing the computer networks/computers for commercial purposes;

15. intentionally disrupting network traffic or crashing the network;

16. stealing data or other intellectual property;

17. posting anonymous messages; and/or

18. engaging in other activities that do not advance the educational purposes for which computer networks/computers are provided.

District personnel, pupils and their parent(s) or legal guardian(s) and authorized non-District users specifically agree to indemnify the school District and school District personnel for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this policy.

Compliance with Children's Internet Protection Act

As a condition for receipt of certain Federal funding, the school District has technology protection measures for all computers in the school District, including computers in media centers/libraries, that block and/or filter material or visual depictions that are obscene, child pornography and harmful to minors as defined in 2, 3, 4, 5, 6, and 7 above and in the Children's Internet Protection Act. The school District will certify the schools in the District, including media centers/libraries are in compliance with the Children's Internet Protection Act and the District complies with and enforces Policy and Regulation 2361.

Compliance with Neighborhood Children's Internet Protection Act

Policy 2361 and this Regulation establish an internet safety protection policy and procedures to address:

1. access by minors to inappropriate matter on the internet;

2. the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

3. unauthorized access, including "hacking" and other unlawful activities by minors online;

4. cyberbullying;

5. inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;

6. unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and

7. measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding the material or visual depictions defined in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Superintendent or designee shall determine internet material that is inappropriate for minors.

Software Libraries on the Network

Software libraries on or through the school District's networks are provided to District personnel, pupils, and non-District authorized users as an educational resource. District personnel, pupils, and non-District authorized users may not install, upload, or download software without the expressed consent of appropriate school District personnel. Any software having the purpose of damaging another person's accounts or information on the school District's computer networks/computers (e.g., computer viruses) is specifically prohibited. School District personnel reserve the right to refuse posting of files and to remove files. School District personnel further reserve the right to immediately limit usage or terminate the District personnel's, pupil's, and non-District authorized users' access or take other action consistent with the Board's policies and regulations of ~~a~~ District personnel, pupils, and non-District authorized users who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer networks/computers without authorization. Pupils and teachers may download copyrighted material for their own use in accordance with Policy and Regulation 2531 - Use of Copyrighted Materials. Pupils and teachers may only redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author or authorized source.

Public Posting Areas (Message Boards, Blogs, Etc.)

Messages are posted from systems connected to the internet around the world and school District personnel do not have total control of the content of messages posted from these other systems. To best utilize system resources, the Superintendent or designee will determine message boards, blogs, etc. that are most applicable to the educational needs of the school District and will permit access to these sites through the District computer networks. The Superintendent or designee may remove messages that are deemed to be unacceptable or in violation of Board policies and regulations. The Superintendent or designee further reserves the right to immediately terminate the access of a pupil who misuses these public posting areas.

Real-time, Interactive, Communication Areas

The Superintendent or designee reserves the right to monitor and immediately limit the use of the computer networks, computers, PEDs and technology resources or terminate the access of District personnel, pupils, and non-District authorized users who misuses real-time conference features (talk/chat/internet relay chat).

Electronic Mail

Electronic mail ("email") is an electronic message sent by or to a person in correspondence with another person having internet mail access. The school District may or may not establish pupil email accounts. In the event the District provides email accounts, all messages sent and received on the school District computer networks/computers must have an educational purpose and are subject to review. Messages received by a District-provided email account are retained in accordance with State and Federal retention regulations. Pupils are expected to remove old messages within fifteen days or school District personnel may remove such messages. The Superintendent or designee may inspect the contents of emails sent by a pupil to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the policy, regulation, or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, State, or Federal officials in any investigation concerning or relating to any email transmitted or any other information on the school District computer networks/computers.

Storage Usage

The District reserves the right to establish maximum storage space that District personnel and pupils receive on the school District's system. District personnel and pupils who exceeds their quota of storage space will be advised to delete files to return to compliance with the predetermined amount of storage space. District personnel and pupils who remain in noncompliance of the storage space allotment after seven school days of notification may have their files removed from the school District's system.

Security

Security on any computer system is a high priority, especially when the system involves many users. If an authorized user (which includes District personnel, pupils, and non-District authorized users) identifies a security problem on the computer networks, computers, PEDs or technology resources, the user must notify the building Principal or appropriate supervisory staff. Authorized users should not inform other individuals of the security problem. Passwords provided to authorized users by the District for access to the District's computer networks, computers, PEDs or technology resources or developed by the authorized user for access to an internet site should not be easily guessable by others or shared with others. Attempts to log in to the system using another authorized user's account may result in termination of the account or access. Authorized users should immediately notify the Principal or designee if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any authorized user identified as a security risk will have limitations placed on usage of the computer networks, computers, PEDs or technology resources or may be terminated as a user and be subject to other disciplinary action.

Vandalism

Vandalism to any school District owned computer networks, computers, PEDs or technology resources may result in cancellation of system privileges and other disciplinary measures in compliance with the District's Conduct-Discipline/Code of Conduct Policy (5500). Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other District computer networks, computers, PEDs and technology resources that are connected to the internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

Printing

The printing facilities of the District's computer networks/computers should be used judiciously. Unauthorized printing for other than educational purposes is prohibited.

Internet Sites

- The District will maintain a website as a communication tool to present up-to-date information to teachers, pupils, parents, the Westfield community, and the global community.

- Administrative offices and curriculum departments will maintain a web page(s) that present up-to-date information about the department, office personnel, function and other related items.

- Individual schools will maintain a website that presents up-to-date information about the school, faculty and staff, upcoming events, news, useful links, and PTO information.

- Extracurricular clubs may establish a web page with the approval of the building principal. Material presented must be pupil produced and relate specifically to the club's activities. The web page must include the following notice: *This is a student extracurricular club web page. Opinions expressed on this page shall not be attributed to the Westfield Public Schools.*

- Website pages must adhere to the parent non-consent form responses regarding the posting of pupils' personal identifying information such as name, photos, and sample of work.

Violations

Violations of the Acceptable Use of Computer Networks, Computers, PEDs and Technology Resources Policy and Regulation may result in a loss of access as well as other disciplinary or legal action.

Disciplinary action shall be taken as indicated in Policy and/or Regulation, 2361 - Acceptable Use of Computer Networks, Computers, Personal Electronic Devices and Technology Resources, Conduct-Discipline/Code of Conduct (5500), Suspension (5610) and Expulsion (5620) as well as possible legal action and reports to the legal authorities and entities.

Determination of Consequences for Violations

The particular consequences for violations of this Policy shall be determined by the Principal or designee. The Superintendent or designee shall determine when school expulsion is the appropriate course of action.

Individuals violating this Policy shall be subject to the consequences as indicated in Board Policy and Regulation 2361; Conduct Discipline/Code of Conduct (5500); Suspension (5610); and Expulsion (5620) and other appropriate discipline, which includes but is not limited to:

1. use of computer networks/computers only under direct supervision;
2. suspension of network privileges;
3. revocation of network privileges;
4. suspension of digital privileges;
5. revocation of digital privileges;
6. suspension from school;
7. expulsion from school; and/or
8. legal action and prosecution by the authorities.

In Effect: December 7, 1999
Revised: December 6, 2005
Revised: June 12, 2012
Revised: August 26, 2014
Reviewed: November 10, 2015
Reviewed: May 10, 2016
Reviewed: May 26, 2020