R 2361 ACCEPTABLE USE OF COMPUTER NETWORKS/ COMPUTERS AND RESOURCES

A Guideline to the Terms and Conditions for Computer/Internet Use

Overview:

The Jefferson Township Public School District provides computer equipment, computer services, and Internet access to its pupils ~~students~~ and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination, and the use of global communication resources.

For the purpose of this Policy and Regulation, "computer networks/computers" includes, but is not limited to, the school district's computer networks, computer servers, computers, other computer hardware and software, Internet equipment and access, and any other computer related equipment.

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

Due to the complex association among government agencies and networks/computers and the requirement 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 ~~the~~ parents/guardians of pupils are aware of their responsibilities. The school district may modify these regulations at any time. The signatures of the pupils and parents/guardian on a district-approved Internet User Contract are legally binding and indicate ~~t~~ the parties have read the terms and conditions carefully, understand their significance, and agree to abide by the rules regulations established under Policy and Regulation 2361.

Pupils are responsible for acceptable and appropriate behavior and conduct when using school district computers networks/computers. Communications on the computer networks/computer are often public in nature and policies and regulations governing appropriate behavior and communications apply. The school district's networks, Internet access, and computers are provided for pupils to conduct research. Access to networks/computers is given only to pupils who agree to act in a

considerate, appropriate, and responsible manner. Parent/guardian permission is required for a pupil to access the school district's computer networks/computers. Access entails responsibility and individual users of the district computer networks/computers are responsible for their behavior and communications over the computer networks/computers. 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 who violate the policies and regulations of the Board.

Computer networks/computer storage areas may be treated in the same manner as other school storage facilities such as school lockers. 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.

The following prohibited behavior and/or conduct using the school district's networks/computers includes but is not limited to, the following:

- Using the computer network(s)/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, court decisions, 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 communications vehicles;
- Intentionally or unintentionally disrupting network traffic or crashing the network;
- Degrading or disrupting equipment or system performance;
- Using circumventing software to bypass security or firewalls;
- Stealing data or other intellectual property;
- Gaining or seeking unauthorized access to resources, entities, or network;
- Forging electronic mail;
- Using an account or password owned by others;
- Invading the privacy of others;
- Posting anonymous messages;
- Possessing any data which are a violation of this policy;
- Engaging in any activity that does not advance the educational purposes for which the computer network/computers are provided;
- Sending or displaying offensive messages or pictures;
- Using obscene language and/or accessing material or visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;

- Using or accessing material or visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;
- 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;
- 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;
- Harassing, insulting, or attacking others;
- Cyber-bullying;
- Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;
- Damaging computers, computer systems, or computer networks;
- Violating copyright laws;
- Trespassing in another person's folders, work, or files;
- Intentionally wasting limited resources;
- Employing the computer network, computer, or Internet for fraud, commercial purposes, financial gain, personal business, product advertisement, or political lobbying (including student body elections).

Violations may result in a loss of access as well as other disciplinary or legal action. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior (in addition to District level penalties).

INTERNET SAFETY

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 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 and World Wide Web;

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. Cyber-bullying;

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 Board shall determine Internet material that is inappropriate for minors.

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 protection 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.

Information Content and Uses of the System:

Pupils may not publish on or over the system any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane, or sexually offensive to a reasonable person, or which, without the approval of the Superintendent or designated school district personnel, contains any advertising or any solicitation to use goods or services. A pupil cannot disclose or post personal contact information about themselves or other people (address, telephone number, etc.). A pupil cannot use the facilities and capabilities of the system to conduct any business or solicit the performance of any activity, which is prohibited by law.

Because Jefferson Township Public Schools provide, through connection to the Internet, access to other computer systems around the world, pupils and their parents/guardians should be advised the Board and school district personnel have no 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 pupils access to Internet resources through the district's computer networks/computers with installed appropriate technology protection measures, parents and pupils must be advised potential dangers do remain and offensive material may be accessed notwithstanding the technology protection measures taken by the school district.

Pupils and their parents/guardians 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. Parents/guardians 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 the termination of such pupil's accounts or access on the school district's computer networks and their independent use of computers.

On-line Conduct and Expectations:

Any action by a pupil or other user (member) of the school district's computer networks/computers that is determined by school district personnel to constitute an inappropriate use of school district's computer networks/computers or to improperly restrict or inhibit other persons from using and enjoying those resources is strictly prohibited and may result in termination of the offending person's access and other consequences in compliance with Board policy and regulation. The user specifically agrees not to submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information, or software in violation of any local, State, or Federal law is also prohibited and is a breach of the Terms and Conditions.

Pupils and their parents/guardians specifically agree to indemnify the Jefferson Township Public School District and school district personnel for any losses, costs, or damages, including reasonable attorney's fees incurred by the Board relating to, or arising out of any breach of this section by the pupil.

Network resources are to be used by the pupil for his/her educational use only; commercial uses are strictly prohibited.

Software Libraries:

Software is provided to pupils as a curricular resource. No pupil may install, upload, or download software, without the expressed written consent of the appropriate school district personnel. Any software having the purpose of damaging another person's account or information on the school district computer networks/computers (example: computer viruses) is specifically prohibited. School district personnel further reserve the right to refuse the posting of files. Additionally, files may be removed at any time without notice. School district personnel further reserve the right to immediately terminate the account or take action consistent with the Board's policy and regulations of a pupil who misuses the software libraries.

Copyrighted Material and Plagiarism:

Copyrighted material must not be placed on any system connected to the network without authorization. Pupils may download copyrighted material for their own use in accordance with Policy and Regulation 2531 Use of Copyrighted Materials. A pupil 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.

Disk Storage:

The district reserves the right to establish maximum storage space a pupil receives on the school district's system. A pupil who exceeds his/her quota of storage space will be advised to delete files to return to compliance with the predetermined amount of storage space. A pupil who remains in non-compliance of the storage space allotment after seven 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 a pupil identifies a security problem on the computer networks/computers, the pupil must notify the appropriate district staff member. The pupil should not inform other individual of a security problem. In order to maintain proper system security, a member must not let others know his/her password, as this would allow others access to his/her account. Passwords provided to pupils by the district for access to the district's computer networks/computers or developed by the pupil for access to an Internet site should not be

easily guessable by others or shared with other pupils. Attempts to log in to the system using another pupil's or person's account may result in termination of the account or access. Pupils 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 pupil identified as a security risk will have limitations placed on usage of the computer networks/computers or may be terminated as a user and be subject to other disciplinary action. Users may not maintain accounts upon graduation or ~~of~~ leaving Jefferson Township Public Schools.

Vandalism:

Vandalism to any school district owned computer networks/computers may result in cancellation of system privileges and other disciplinary measures in accordance with the district's discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other networks that are connected to the Internet backbone or of doing intentional damage to hardware or software resident on the system. This includes, but is not limited to, the uploading or creation of computer viruses and unauthorized entry into the network or system.

Printing:

The printing facilities of the Jefferson Township Public School network should be used judiciously. Unauthorized printing is a drain of the capacity of the networks, adds expense, and shortens the life of equipment.

Electronic Mail: (as available)

Electronic mail (also referred to as "mail" or "e-mail") is an electronic message that is sent by or to a person in correspondence with another person having Internet mail access. Users are expected to delete read messages in a timely fashion; it should be noted that system administrators may delete messages not erased in a timely fashion. Additionally, e-mail messages may be inspected for content, and users should not consider these messages as private. The system administrators may inspect the contents of mail sent by one member to an identified addressee, and disclose such content to other than the sender or intended recipient, without the consent of the sender or identified recipient, in order to comply with the law and/or policies of the Jefferson Township Public School District, or to investigate complaints regarding mail which is alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material. Jefferson Township Public Schools reserve the right to cooperate fully with local, state, or federal officials in any investigation concerning or relating to any mail transmitted on the Jefferson Township Public School network. In summary, users should not expect that

all files or e-mail stored on District servers will always be private. Pupil users will have internal e-mail addresses; staff members will have e-mail addresses which can be used to send mail outside of the local network.

Game-Playing:

Pupils are not permitted to use district devices, networks, or resources for non-educational game playing unless specifically permitted by their teacher.

~~Game playing is permitted at the Elementary School level only when terminals are not needed for other purposes and has been approved by the teacher. Game playing over dial-up links or other inter-machine communication is prohibited.~~

~~Game playing is not permitted in the Middle School or High School at any time.~~

Public Posting Areas (Message Boards/UseNet Groups): (as available)

UseNet messages are posted from systems connected to the Internet from around the world. It should be noted that the Jefferson Township Public School District's system administrators have no control over the content of messages posted from these other systems. To best utilize system resources, the system administrators will determine which UseNet groups are most applicable to the curricular needs of the school District and may carry these groups on the local system. The system administrators, at their sole discretion, may remove messages posted locally that are deemed to be unacceptable or in violation of the Terms and Conditions. The system administrators, at their sole discretion, further reserve the right to immediately terminate the account of a member who misuses the message boards or UseNet groups.

Internet User Contract:

Google Chrome is an integrated part of Chromebooks and Google's Chrome operating system. ~~Internet Explorer is an integrated part of the Windows operating system.~~ While the Jefferson Township Public School District and the system administrators attempt to restrict pupil usage of the Internet, it is understood that each user is responsible for his or her own actions.

In order for pupils ~~students~~ to use any machine connected to the Internet, pupil and parent/guardian must sign a User Contract.

District Indemnity:

The District makes no warranties of any kind expressed or implied for the Internet service and is indemnified against any damage caused by a pupil's ~~student's~~ inappropriate use of the system (i.e., loss of data, financial charges), and may recoup any losses directly from the pupil or the pupil's parent or guardian. In addition, the District denies any responsibility for the accuracy and quality of the information obtained through the Internet system.

Note: The Jefferson Township Public School District provides network firewall and content filtering services through a network security appliance compliant to State and Federal regulations.

Issued: 18 September 2012
Revised: 21 July 2025