# East Penn School District

## Acceptable Use Policy

Acceptable Use of Technology Resources, Electronic Communications and Information Systems

No. 138.1

| | |
|---|---|
| Book | Policy Manual |
| Section | 100 Programs |
| Title | Acceptable Use of Technology Resources, Electronic Communication and Information Systems |
| Number | 138.1 |
| Status | Active |
| Legal | 1. 24 P.S. 1317.1<br>2. Pol. 611<br>3. 17 U.S.C. 101 et seq<br>4. Pol. 814<br>5. Pol. 218<br>6. Pol. 233<br>7. Pol. 317<br>8. Pol. 417<br>9. Pol. 517<br>20 U.S.C. 1232g<br>20 U.S.C. 6777<br>22 PA Code 403.1<br>24 P.S. 4601 et seq<br>47 U.S.C. 254 |
| Adopted | August 25, 1997 |
| Last Revised | August 13, 2007 |

## Purpose

The East Penn School District supports the use of technology, information systems, and the Internet for educational purposes and in the performance of job responsibilities. The use of technology resources must be consistent with the educational and administrative objectives of the school district. Personal or unacceptable use of technology resources as hereinafter defined is prohibited and may result in the cancellation of use and appropriate disciplinary actions.

## Authority

The school district's systems must be used solely for education-related purposes and performance of school district job duties. Unacceptable use includes intentionally accessing **inappropriate material**, defined as, but not limited to, visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that advocates the destruction of property or is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color,

religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability) violent, bullying, or terroristic.

Access to the school district's computing facilities, network, electronic communications, informational systems and other technology resources is a privilege, not a right. Technology resources, user accounts and information are the property of the school district, which reserves the right to access any user accounts at any time to ensure compliance with this policy and to deny access to prevent unauthorized, inappropriate or illegal activity or use, and may revoke those privileges and/or administer appropriate disciplinary action. The school district will cooperate to the extent legally required with the Internet Service Provider (ISP) and local, state and federal officials in any investigation concerning or related to the use or misuse of the technology systems, and/or violation of applicable laws or regulations.

Employees' and students' personal technology devices brought onto the school district's property or that are present at school district events or connected to the school district's network or containing school district or student data, or school district procured software programs may also be inspected and/or accessed to ensure compliance with this policy and other school district policies, to protect the school district's resources, and to comply with the law. Users may not use their personal computers to access the school district's intranet, Internet or any other technology resources unless approved by the Superintendent of Schools or his/her designee, either individually, by policy, or by written procedure. The school district intends to strictly protect its technology systems against outside and internal risks and vulnerabilities. Consequently, users are required to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent of Schools or his/her designee.

The Director of Information Technology or his/her designee may access user accounts in order to perform routine maintenance and security tasks. Users have no privacy expectation in the contents of their personal files or any of their use of the school district's systems. The school district has the responsibility to monitor, track and/or log system use to maintain security and to allocate fileserver space.

Measures designed to restrict adults' and minors' access to material harmful to minors may be temporarily disabled to enable an adult or student to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose, with permission of the Superintendent.

## **Delegation of Responsibility**

School District –

The Superintendent of Schools or his/her designee has the responsibility to provide for systems and procedures to monitor, track, log, access and report sufficient aspects of its systems technology, and related systems may be inspected pursuant to provisions of applicable law, to ensure compliance with this policy and other school district policies, to protect the school district's resources, and to comply with the law. The systems may include personal computers, network, Internet, electronic communication systems, and media brought onto the school district's property or at school district events, potentially containing school district programs or school district or student data (including images, files, and other information).

The Superintendent of Schools or his/her designee is responsible for defining and setting usage limits or quotas to ensure optimal use of the system according to the following priorities:

1. Uses that directly support the academic activities of the students.

2. Uses that indirectly benefit the education of the student, such as researching college

information.

The Superintendent of Schools or his/her designee is responsible for ensuring the security of personal and confidential data maintained in employee or student information management systems. In systems not maintained by the district on district equipment, the Superintendent is responsible for periodic auditing to ensure adequate security measures are in place. It is the express responsibility of all users to be aware of confidentiality rights governing such data, and to protect the data. All such data not stored on servers shall be encrypted.

The Superintendent of Schools or his/her designee additionally reserves the right to:

1. View and monitor network traffic, fileserver space, processor and system utilization, and all applications provided through the network and communications systems, including e-mail.

2. Maintain e-mail and fileserver quotas.

3. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and/or any other applicable school district policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of school district resources and equipment.

4. Determine which technology services will be provided through school district resources.

The Director of Information Technology or his/her designee will serve as the coordinator to oversee the school district's technology systems and will work with district, regional or state organizations to educate employees, approve activities, provide leadership for proper training in the use of the systems and the requirements of this policy, establish a system to ensure adequate supervision of the technology systems, maintain executed user agreements, and interpret and enforce this policy.

The Director of Information Technology or his/her designee will maintain a procedure for creating and assigning individual and class accounts, set quotas for disk usage on the system, establish a data file retention schedule, and maintain the school district virus protection process.

User –

All users are expected to adhere to the requirements of this policy. All users are responsible for respecting the rights of other users within the school district and school district technology systems, to abide by the rules published by the school district and its Internet Service Provider (ISP) and to obey local, state and federal laws.

Users shall abide by generally accepted rules that include but are not limited to the following:

1. Be polite. Do not become abrasive in messages to others. General school district discipline code rules and policies for behavior and communicating apply.

2. Use appropriate language in network communications. Do not swear or use vulgarities or other inappropriate or harassing language.

3. Do not reveal the personal addresses or telephone numbers of others.

4. Recognize that e-mail is not private or confidential. Do not transmit private or confidential information via e-mail unless the information is encrypted before transmission.

5. Do not use the technology resources in any way that would interfere with or disrupt its use by other users.

6. All non-copyrighted communications and information placed by the author on the district web site become the property of the school district. Copyrighted material shall not be placed on the district web site without permission of the author.

7. Respect the rights of other users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, creed, ethnicity, age, marital status or handicap status.

**Guidelines**

Access to the System

System accounts will be made available according to school district procedures developed by the Director of Information Technology or his/her designee.

This policy, as well as other relevant school district policies, will govern use of the school district's technology systems.

Parental/Guardian Notification and Responsibility

The school district shall provide a copy of this policy at the beginning of each school year to parents/guardians, students, and employees. The school district encourages parents/guardians to review this policy and discuss with their child(ren) what material is and is not acceptable for their child(ren) to access in school through the school district's technology systems. Users are required to sign and agree to the district's acceptable use policy and Internet Access Acknowledgement Form.

School District Limitation of Liability

The school district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the school district's systems will be error-free or without defect.

The school district does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the school district. The school district shall not be responsible for material that is retrieved through the Internet or the consequences that may result from them.

The school district is neither responsible for nor guarantees the accuracy or quality of the information obtained its systems.

The school district shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed or unavailable when using the computers, network and electronic communications systems.

The school district shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the school district's systems. In no event shall the school district be liable to the user for any damages whether direct, indirect, special or consequential, arising from the use of the systems.

Prohibitions

The use of the school district's systems for illegal, inappropriate, or unacceptable purposes as designated by this policy by anyone is prohibited. The Superintendent of Schools or his/her designee reserves the right to determine if any activity constitutes an acceptable or unacceptable use of the technology systems. The prohibitions on unacceptable use are in effect at all times.

Students are prohibited from using their personal computers on school district premises and property, at school district events, or through connection to the school district technology systems, unless permission has been granted by the Superintendent of Schools or his/her designee.

Students who are performing volunteer fire company, ambulance or rescue squad functions, or need such a computer due to their medical condition, or the medical condition of a member of their family, with prior notice and the approval of the Superintendent of Schools or his/her designee, may qualify for an exemption of this prohibition.[1]

All users are prohibited from using school systems to:

1. Send, receive, view, download, access, or transmit inappropriate matter and material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, obscene, sexually explicit, lewd, hateful, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, vulgar, rude, inflammatory, threatening, profane, pornographic, terroristic and/or illegal.

2. Gamble.

3. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.

4. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (online, real-time conversations).

5. Facilitate any illegal activity.

6. Mass mail non-educational or non-work related information (for example: the use of the "everyone" distribution list, building level distribution lists, or other e-mail distribution lists to offer personal items for sale).

7. Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable school district policies) or conduct unauthorized fundraising or advertising on behalf of the school district or non-school district organizations. **Commercial purposes** are defined as offering or providing goods or services or purchasing goods or services for personal use. School district acquisition policies will be followed for school district purchase of goods or supplies through the school district system.[2]

8. Political lobbying for the purpose of electing public officials.

9. Install, distribute, reproduce or use copyrighted software not licensed by the district on school district computers, or copy school district software to unauthorized computer

systems, intentionally infringing upon the intellectual property rights of others or violating a copyright (see the section on copyright infringement in this policy).

10. Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on school district computers is restricted to the Director of Information Technology or his/her designee.

11. Encrypt messages using encryption software that is not authorized by the school district from any access point on school district equipment or school district property.

12. Access, interfere with, possess, or distribute confidential or private information unless within the scope of the position's responsibility. Example: Accessing other students' accounts to obtain their grades.

13. Use the systems to send any school district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the school district's business or educational interests.

14. Post personal or professional web pages without administrative approval.

15. Post or transmit anonymous messages.

16. Utilize district equipment for conducting denial of service attacks on the district or other systems.

Access and Security

Users must immediately notify the Director of Information Technology or his/her designee if they have identified a possible security problem or inadvertently accessed inappropriate material. The following activities related to access to the school district's technology systems and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.

2. Acquiring or attempting to acquire passwords of another user.

3. Altering a communication originally received from another person or computer with the intent to deceive.

4. Using school district resources to engage in any illegal act, including but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, or being involved in a terroristic threat against any person or property.

5. Disabling, circumventing or attempting to defeat any school district security measure, program or device, including, but not limited to, anti-spyware, anti-spam, and virus protection software or procedures.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interfering with or disrupting the technology systems, network accounts, services or

equipment of others, including, but not limited to, the propagation of computer worms and viruses, Trojan Horse and trapdoor program code, and the sending of electronic chain mail. The user may not hack or crack the network or others' computers, whether by hardware, software, parasiteware, viruses and worms or other hardware or software designed to obtain information or damage the technology systems or any component of the network, and may not strip or harvest information, or take control of any computer without permission.

2. Altering or attempting to alter other users' or system files, system security software or the systems themselves, except for Information Technology staff in the performance of their duties.

3. Scanning of the technology systems for security vulnerabilities without authorization.

4. Attempting to alter any school district computing or networking components (including, but not limited to fileservers, bridges, routers, or hubs) without authorization.

5. Using routers or switches, or configuring wireless technology, attempting to create network connections, or extending any computer, telephonic device, electronic communications systems, or network services, whether wired, wireless, cable, or by other means, without authorization.

6. Failing to comply with requests from teachers or school district administrators to discontinue activities that the teachers or administrators believe threaten the operation or integrity of the technology systems.

Content Guidelines

Information electronically published on the school district's technology systems shall be subject to the following guidelines:

1. Published documents, including but not limited to audio and video clips or conferences, may not include a child's phone number, street address, box number, or name (other than first name) when associated with other identifying information, such as a picture or the names of other family members, without parent/guardian consent in writing.

2. Documents, web pages, electronic communications, or video conferences may not include personally identifiable information that indicates the specific physical location of a student at a given time without parent/guardian consent in writing.

3. Documents, web pages and electronic communications must conform to all school district policies and guidelines.

Expectation of Privacy

Users' violations of this policy, any other school district policy, or the law may be discovered by routine maintenance and monitoring of the school district systems. Users waive all expectation of privacy in their usage of the systems.

Copyright Infringement and Plagiarism

Federal laws, cases and guidelines pertaining to copyright will govern the use of material accessed through school district resources. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements.[3][4]

Selection of Material

When using the Internet or other technology resources for class activities, teachers shall select material that is appropriate to the age of the students and is relevant to the course objectives. Teachers must preview the materials and web sites they require or recommend students to access to determine the appropriateness of the material contained on or accessed through the web site. Teachers shall provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly.

Safety and Privacy

The school district will take reasonable measures to protect users from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately inform the Superintendent of Schools or his/her designee.

Students will not post personal contact information about themselves or other people on the technology systems. District systems and devices shall not be used to invade the privacy of any person.

District system users may not disclose, use or disseminate confidential or personal student or employee information including, but not limited to, grades, social security numbers, home addresses and telephone numbers, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the school district unless authorized to do so.

Consequences for Inappropriate, Unauthorized and/or Illegal Use

Students and employees are hereby made aware that violations of this policy or other related policies or unlawful use of the technology systems may result in loss of technology access and a variety of other disciplinary actions, including, but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions (with or without pay for employees), dismissal, expulsions, and/or legal proceedings on a case-by-case basis.[5][6][7][8][9]

This policy incorporates all other relevant school district policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, property policies, curriculum policies, and improper conduct policies.

The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be financially responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy, which may result in cancellation of access to the school district's technology systems and resources, and is subject to discipline.

Illegal usage of district systems or equipment will be reported to law enforcement authorities.

EAST PENN SCHOOL DISTRICT

# ACCEPTABLE USE POLICY AND INTERNET ACCESS ACKNOWLEDGEMENT FORM

I have read the East Penn School District Acceptable Use of Technology Resources, Electronic Communications and Information Systems Policy and I will comply with its terms. I understand that district technology resources are provided for the purpose of exploring educational topics, conducting research and classroom activities, and communicating with others in support of educational goals and the business of the district.

I understand that the district has the right to review any material stored on any system that the district provides and to edit or remove any material. I acknowledge that my access to such material is a privilege, not a right. I acknowledge that it is impossible for the district to restrict access to all controversial and inappropriate materials, and I will not hold the district responsible for materials acquired on the network.

I understand that violation of this policy may have consequences ranging from revocation of access privileges to district disciplinary actions, and that violations may be reported to local, state, and/or federal legal authorities when applicable.

_____ I am a student _____ I am an employee

Name (please print): _____

Signature: _____ Date: ____/____ /_____

School: _____ Grade: _____ Phone: _____

If above signatory is a minor, a parent or guardian signature is required. By signing below, I (as a parent or guardian) have read the above-mentioned policy and agree that my child and I will comply with its terms. I hereby give permission for my child to access the Internet as an academic resource.

Name (please print): _____

Signature: _____ Date: ____/____ /_____

Phone: _____

*Information Technology, 1/22/2007*
*Revised: May 18, 2007*