Director Procedure Number: DJ121
Title: Acceptable Use of Technology and Internet Safety
Section: Operations

Acceptable Use of Technology and Internet Safety

Guidelines

Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via any electronic device should be assumed to be the property of EASTERN and shall not be disclosed without proper authorization. All users shall respect the privacy of other users.

The computers and computer accounts given to users are to assist them in the performance of their jobs or meeting the requirements of their educational program. Users do not have an expectation to privacy and expressly waive any rights to privacy in anything they create, store, send, or receive on the computer or through the Internet or on the network. Users understand that EASTERN may use human or automated means to monitor use of its technology resources.

Email services will be provided to students who agree in writing to act in a considerate and responsible manner. The parents of all Internet users will be notified of guidelines for student internet use. Students may not disclose or disseminate personal identification information about themselves or others when using the Internet (World Wide Web), email or participate in chat rooms. In compliance with the Children's Internet Protection Act, EASTERN will "…educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response."

Prohibitions

Students and staff are expected to act in a responsible, ethical, and legal manner in accordance with school policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Illegal activity (e.g. violation of licensing agreements, violation of copyright law, theft of services);
2. Commercial or for-profit business;
3. Product advertisement or political lobbying;
4. Is harmful or prejudicial to students; for example, materials which are libelous and obscene as defined by the law of the Commonwealth of Pennsylvania or the United States;
5. Constitutes bullying (including cyber-bullying) or otherwise fosters disruptiveness among the students so as to interfere with the learning environment of EASTERN;
6. Threatens immediate harm to the welfare of the school community or any individual;
7. Discriminates against any segment of the student body or interferes with another's individual rights;
8. Encourages, abets or permits unlawful activity, including the violation of copyright laws;
9. Violates the separation of church and state;
10. Can intentionally cause damage to hardware, software or data;
11. Can gain or attempt to gain access to restricted material or systems;
12. Promotes or permits gambling;
13. Pornographic material or child pornography;
14. Access by students and minors to material that is harmful to minors or is determined inappropriate or inconsistent with the instructional purposes and mission of EASTERN as determined by the Director with the Technology Manager;
15. Intentional, unauthorized obtaining or modifying of files and passwords belonging to another user without the permission of such other user;
16. Impersonation of another user, anonymity, and pseudonyms (excluding the use of user names assigned or approved by EASTERN);
17. Loading or using of games, programs, files, or other electronic media;
18. Posting anonymous messages; or
19. Otherwise violates school rules or Eastern policies.

Etiquette:

Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in messages to others. General EASTERN rules and policies for behavior and communicating apply.
2. Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
3. Do not reveal the personal addresses or telephone numbers of others.
4. Recognize that e-mail is not private or confidential.
5. Do not use technology in any way that would interfere with or disrupt its use by other users.
6. Consider all communications and information accessible via the Internet to be private property.
7. Respect the rights of other users to an open and hospitable technology environment, regardless of one's sex, race, color, national origin or disability.

Incidental Personal Use

Use of EASTERN's technology systems by an individual employee for occasional personal communications must comply with this policy and all other school policies, procedures and rules, as well as ISP, local, state and federal laws and may not interfere with the employee's job duties and performance, with system operations, or with other system users, and must not damage the school's technology systems. Under no circumstances should the employee believe his/her use is private. EASTERN reserves the right to monitor, track, access and log the use of its technology systems at any time.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or school files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network and/or electronic devices at the determination of the Director and Technology Manager.

Blocking software will be used on the Internet to protect minor students from obscene material, child pornography, other visual depictions deemed harmful to minors (as defined by the Children's Internet Protection Act), and other categories deemed necessary by the administration. Other Internet users will also have these categories blocked. An administrator, supervisor, or person authorized by the Joint Committee may disable the technology protection measure if needed for bonafide research or other lawful purpose.

Consequences for Inappropriate Use

All students and staff members will sign the Network Acceptable Use Agreement and comply with EASTERN's standards or lose their access privilege. The Information Services Department regularly monitors unauthorized access or unlawful activity on EASTERN network computers and servers. Inappropriate, unauthorized or illegal use (including hacking or attempted hacking) may result in the cancellation of the offender's privileges. Appropriate disciplinary action may be taken.

The user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of technology, intentional deletion or damage to files of data belonging to others, copyright violations, and theft of services may be reported to the appropriate legal authorities for possible prosecution. Vandalism will result in denial of access privileges. Vandalism is defined as tampering, modification or misuse of technology or any malicious attempt to harm or destroy data from another user, the Internet, technology or other networks. This includes, but is not limited to, uploading or creating computer viruses, denial of service attacks and unauthorized access.

Copyright

Copyright and licensing agreements are to be upheld by all users. The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

Safety

The school will take reasonable efforts to protect users of the network from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report it immediately to a teacher, administrator, or the Technology Manager. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.

Children's Internet Protection Act
Policy J113 Copyright Material

Adopted: 12/11/2013
Updated: 4/9/2025