AW3918

RESOLUTION NO. 08-14

A RESOLUTION OF AMITY TOWNSHIP, BERKS COUNTY, PENNSYLVANIA, ESTABLISHING POLICIES FOR ACCEPTABLE USE OF THE INTERNET FOR EMPLOYEES OF AMITY TOWNSHIP

WHEREAS, Amity Township wishes to establish a written policy to establish regulations for employees use of the internet.

NOW THEREFORE BE IT RESOLVED, by the Board of Supervisors of the Township of Amity, Berks County, Pennsylvania that the Township of Amity hereby adopts the Acceptable Use of Internet Policy as follows, as the official Acceptable Use of Internet for the Township of Amity.

ACCEPTABLE USE OF INTERNET

14.02.01 PURPOSE:

The Board Of Supervisors of Amity Township ("Township") supports use of the Internet and other computer networks in the Township's operational programs in order to facilitate daily operations through interpersonal communications and access to information, research and collaboration.

14.02.02 POLICY:

The availability and use of the personal computers within the work environment have provided many opportunities for enhancement of productivity and effectiveness. If not managed properly, these technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this agency, its members, and the public. Therefore, it is the policy of the Amity Township Police Department and the Township that all members and staff abide by the guidelines set forth herein when using personal computers and the services of both internal and external databases and information exchange networks, and where applicable, voice mail, mobile data terminals, and related electronic messaging devices.

14.02.03 AUTHORITY:

The electronic information available to employees does not imply endorsement by the Township of the content, nor does the Township guarantee the accuracy of information received. The Township shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The Township shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The Township reserves the right to log network use and to monitor fileserver space utilization by all Township users, including the Police Department.

The Township establishes that network use is a privilege and not a right. Inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action up to and including termination.

The Board of Supervisors may establish a list of materials, in addition to those stated in law and this Policy, that are inappropriate for access by employees.

14.02.04 DEFINITIONS:

Electronic Messaging Device (EMD): For purposes of this policy, electronic messaging devices include personal computers, laptop computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards and Internet services, mobile data terminals, cellular phones, and facsimile transmissions.

System Administrator: For purposes of this policy, the System Administrator is the Township Manager and is designated with the responsibility for managing all aspects of any EMD.

Personal Computer: Any agency or personally owned computer that provides access to the agency or agency personnel. This includes both on and off duty usage.

14.02.05 DELEGATION OF RESPONSIBILITY:

The Township shall make every effort to ensure that the Internet is a resource that is used responsibly by employees.

The Township Manager shall have the authority to determine what is inappropriate use. Use of the Internet by any employee is consent to the Township Manager's authority over the determination of inappropriateness.

The Township Manager shall be responsible for implementing technology and procedures to determine whether the Township's computers are being used for purposes prohibited by law or for accessing sexually explicit materials, except as necessary for a Chief of Police approved investigation. Any investigation in this regard shall be communicated to the Township Manager to be certain that he is aware of the investigation, but not the subject nor purpose of the investigation. The Township may impose limitations that include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, or constitute child pornography.

2. Maintaining and securing a usage log.

3. Preparing additional guidelines beyond this Policy.

14.02.06 PROCEDURES FOR NETWORK ACCOUNTS:

Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system. Employees are expected to act in a responsible, ethical and legal manner in accordance with this Township policy, accepted rules of network etiquette, and federal and state law.

A. General

1. The following procedures apply to all media which are:

a. Accessed on or from departmental premises;

b. Accessed using department or personal computer equipment or department paid access methods;

c. Communications that make reference to the department in a manner; and/or

d. Used in a manner that identifies the employee with the department

2. Transmission of electronics messages and information on communications media provided for employees of the agency shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence, or verbal communication.

3. This agency encourages authorized and trained personnel with access to EMDs to utilize these devices whenever necessary. However, use of any these devices is a privilege that is subject to revocation.

4. EMDs and their contents are the property of this agency and intended for use in conducting official business.

5. Members are advised that they do not maintain any right to privacy in EMD equipment or its contents.

   a. This agency will monitor information contained in EMDs and may require members to provide passwords to files that have been encrypted or password protected, including voice mails.

   b. The agency shall access, for quality control purposes, for violations of this policy, or any reason whatsoever, electronic and voice transmissions of members.

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

   a. Employees shall not reveal their passwords to another individual.

   b. Users are not to use a computer that has been logged in under another employee's name.

c. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

7. Computer repairs shall be made by agency authorized and approved sources by the Township only. At no time may employees effectuate repairs without the prior written consent of the Township.

8. Accessing or transmitting materials (other than that required for police business) that involves the use of obscene language, images, jokes, sexually explicit materials, or messages or information that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

9. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or networked systems) only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes but is not limited to the following:

   a. Transmittal of misconduct, disciplinary information, medical records, or related information

   b. Criminal history information and confidential informant master files, identification files, or related information.

   c. Intelligence files and information containing sensitive tactical and undercover information.

   d. Employment related matters such as grievances, contracts, or other information shall not be conducted on Township computers or EMDs.

10. Employees may not attempt to read or "hack" into other systems or logins; "crack" passwords; breach computer or network security measure; or monitor electronics filings or communications of other employees or third party except by explicit direction of the Chief of Police or Township Manager.

11. No E-mail or other electronics communications may be sent that attempts to hide the identity of the sender or represents the sender as someone else or some other agency.

12. Media may not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

13. Employees may not copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner or except for a single copy of reference. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

14. No member shall access or allow others to access any file or database unless that person has a need and a right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.

15. An EMD is designed and intended to conduct business of this agency and is restricted to that purpose and that purpose only. Installation of or access to software for purely entertainment or personal or outside business purposes is prohibited.

B. Importing/Downloading Information and Software

1. Employees shall not download or install on their EMDs or network terminal any file (including sound and video files and file attached to E-mail messages), software, or other materials from the Internet or other external sources.

2. Members shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

3. Members shall observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.

4. Members shall not permit unauthorized persons to use this agency's electronic mail system.

5. To avoid breaches of security, members shall log off any personal computer that has access to the agency's computer network,

electronic mail system, the Internet, or sensitive information whenever they leave their workstation.

14.02.07 CONSEQUENCES FOR INAPPROPRIATE USE

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network, intentional deletion or damage to files of data belonging to others, copyright violations, and theft of services or copying of any materials on the Township system for personal or other use, or any other violations of this policy shall be reported to the appropriate legal authorities and/or the Township Manager for possible prosecution and disciplinary action. Disciplinary action for violation of this policy shall mean all discipline up to and including termination of employment.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use. Vandalism will result in cancellation of access privileges and other disciplinary action.

Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

14.02.08 SAFETY

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to the Township Manager. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.

Any Township computer/server utilized by employees may be equipped with Internet blocking/filtering software.

AW3918

I acknowledge that I have read the Amity Township Acceptable Use of Internet Policy and agree to the terms and conditions.

_____

Signature

_____

Name (printed)

AW3918

DULY ADOPTED AND APPROVED this _____ day of November, 2008.

BOARD OF SUPERVISORS
TOWNSHIP OF AMITY

Kim McGrath

Paul R Weller

Robert B. Lyne

Scott Stump

Attest: _____
Secretary

Approved this 19 day of November, 2008.

I certify that this is a true and correct copy of a Resolution, duly adopted by the Township of Amity, Berks County, Pennsylvania on November 19, 2008.

_____
Secretary