

# PEOPLE'S PLACE

## Internet and Email Policy

Approved By: Board of Directors  
Review/Revision Date: 02/01/2009

### I. PURPOSE

The purpose of this policy is to maintain systems and conduct activities that provide information and service integration.

### II. POLICY STATEMENT

It is the policy of People's Place to ensure that use of e-mail and the internet among staff and volunteers is consistent with our policies, all applicable laws, and the user's job responsibilities.

### III. APPLICATION

This policy applies to all People's Place staff and volunteers.

### IV. DEFINITIONS

None.

### V. STANDARDS

- A. Internet use shall be limited to company business not personal use as it could result in extensive damage to our computer systems. The Internet must not be used to access, create, transmit, print or download material that is derogatory, defamatory, obscene, or offensive, such as slurs, or anything that may be construed as harassment or disparagement based on color, race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.
- B. No backgrounds or wallpaper should be installed other than what is available through the Windows operating system.
- C. E-mail is not private and messages relating to or supporting illegal activities will be reported to authorities. Employees are prohibited from sending e-mail messages that may be considered offensive, hostile, aggressive, threatening, or inappropriate to anyone. Also, employees are prohibited to search, print, post, view, or display any pornographic, adult or any other material that may be inappropriate.
- D. E-mails should be deleted that are not expected, that are from someone you do not know or are suspicious in any way. Never open any attachments to these e-mails.
- E. Downloading or disseminating of copyrighted material that is available on the Internet is an infringement of copyright law. Permission to copy the material must be obtained from the publisher.

- F. Each individual may request to change his or her e-mail password by contacting the administration office. The only person with the authority to change another's password is the Administrator-who will do so at the request of the user involved (e.g., in the event that a user should forget his or her password and be unable to gain access to his or her own e-mail account).
- G. The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The administrator may close, deny, revoke or suspend an account at any time.
- H. Network Etiquette-Employees are to abide by the generally accepted rules of network Etiquette.
  - 1. Be polite. Do not get abusive in your messages to others.
  - 2. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
- I. An individual who violates any provision(s) of this policy and causes damage to computers or systems will be responsible for the cost of repairs, reconfiguration, or restoration. The employee may also be subject to disciplinary action up to and including termination.
- J. Time sensitive information should be supplemented with an alternative form of communication.

**VI. REFERENCES**

None.

**VII. EXHIBITS**

- A. Delaware Code – Provisions for Computer Crime

Delaware Code – Provisions for Computer Crime

Title 11, Chapter 5, Section 932. Unauthorized access.

A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization. (64 Del. Laws, c. 438,1.)

Title 11, Chapter 5, Section 933. Theft of computer services.

A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services, computer software or data. (64 Del. Laws, c. 438,1.)

Title 11, Chapter 5, Section 934. Interruption of computer services.

A person is guilty of the computer crime of interruption of computer services when that person, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system. (64 Del. Laws, c. 438,1.)

Title 11, Chapter 5, Section 935. Misuse of computer system information.

A person is guilty of the computer crime of misuse of computer system information when:

- (1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system;
- (2) That person intentionally or recklessly and without authorization:
  - a. Alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system; or
  - b. Interrupts or adds data to data residing within a computer system;
- (3) That person knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this section; or
- (4) That person uses or discloses any data which that person knows or believes was obtained in violation of subdivision (1) or (2) of this section. (64 Del. Laws, c. 438,1.)

Title 11, Chapter 5, Section 936. Destruction of computer equipment.

A person is guilty of the computer crime of destruction of computer equipment when that person, without authorization, intentionally or recklessly tampers with, takes, transfers, conceals, alters, damages or destroys any equipment used in a computer system or intentionally or recklessly causes any of the foregoing to occur. (64 Del. Laws, c. 438,1.)