# COMPUTER SAFETY AND ACCEPTABLE USE POLICY

Updated 12/23/2020

## PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at Emery Town. These rules are in place to protect both the employee and Emery Town.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Emery Town. This policy applies to all equipment that is owned or leased by Emery Town.

## POLICY

1.1) Employees are responsible for exercising good judgment regarding the reasonableness of personal use of town computer equipment and online resources, and if there is any uncertainty, employees should consult their supervisor or manager.

1.2) Emery Town reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.3) Passwords must be kept confidential.

1.4) All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less.

## 2. UNACCEPTABLE USE

The following activities are strictly prohibited, with no exceptions:

2.3) Access of internet sites which advocate, advertise, solicit, donate, trade, or sell pornography, gambling, human trafficking, illegal substances, weaponry.

2.2) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

2.3) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

2.4) Using an Emery Town computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

2.5) Making fraudulent offers of products, items, or services originating from any Emery Town account.

2.6) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

## 3. EMAIL. SOCIAL MEDIA. AND OTHER COMMUNICATION ACTIVITIES

When using company resources users must realize they are perceived of as representing the company. In all cases – and especially when employees specifically state an affiliation to the company – they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

Additionally, the following activities are strictly prohibited, with no exceptions:

3.1) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

3.2) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3.3) Unauthorized use, or forging, of email header information.

3.4) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

## NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.