

CATEGORIES

DATE PROPOSED: 8/10/18

DATE OF VOTE: 8/10/18

ACCEPT (Y/N): Y

The Municipal Ice Complex (MIC) may, at its discretion, provide computers, laptop computers or other portable computer devices to certain employees for the express purpose of enhancing the productivity and operational efficiency of those employees. This policy establishes guidelines for the usage of such devices.

All employee computer equipment shall be used for the sole and express purpose of conducting official business and maintaining the operations of the facility. Employees are prohibited from using facility computing devices for personal business. Employees may not use facility computing devices for any illegal or unethical purposes or any other activity prohibited by MIC Policy. Doing so may result in termination.

Although issued to an individual employee, all computing devices are considered the property of the MIC and shall be returned upon termination of employment.

Employees shall not install any unapproved software or applications on facility owned computing devices. Approval must be obtained from the Senior Facility Manager (SFM) prior to any new software installation. All facility computers should have an active virus protection program installed and operating at all times. Employees should use caution when downloading files that could contain viruses and malware. If an employee's computing device appears to have a virus or other similar problem, or needs any other repair, the employee should contact the SFM to arrange for repair, rather than seeking repair service on their own.

Employees are expected to take all appropriate measures and precautions to prevent the loss, theft, damage and/or unauthorized use of facility equipment, including, but not limited to:

1. Keep the computing device in a locked and secured environment when not in use. Do not leave the computing device unattended at any time in an unsecured location, such as an unlocked empty office. Keep the computing device in sight at all times while in public places such as airports, restaurants, etc.
2. Do not leave the computing device in a vehicle for an extended period of time, particularly during periods of extreme heat or cold.
3. Keep food and drinks away from all computing devices and work areas.

Should an employee's computing device be lost or stolen or damaged, the employee must immediately report the incident to his/her supervisor and obtain a police report documenting the theft (if applicable). The MIC is under no legal, financial or other obligation to provide a replacement device for any employee whose device is lost, damaged or stolen.

The MIC may add security and other tracking technology to any and all computing devices issued by it. Any and all usage of MIC computer devices is subject to management review, monitoring and auditing by the facility.