## Technology Use Policy

The popularity and use of technology have advanced significantly in recent years. While technology can be a valuable tool both in and out of the workplace, it poses significant risks for the Association and its employees if not used properly. This policy governs the use of technology by Association employees. Where no policy or guideline exists or if there are any questions regarding this policy, consult with the Human Resources Department.

Employees may not useAssociation-owned or personal computer systems/telecommunications devices, social media, or any electronic communications such as email in a manner that violates Association policies, including, but not limited to, the following policies as stated in the *Employee Advisory Handbook and Guidelines:*

* Hours of Work
* Employee Responsibility
* Workplace Privacy
* Anti-discrimination
* Anti-harassment
* Violence in the Workplace Prevention
* Disciplinary Action
* Overtime

Social media for the purposes of this policy is defined as online platforms that allow for direct interaction and participation among people. This includes, but is not limited to, social networking websites (i.e. Facebook, Myspace, LinkedIn, YouTube, Digg); blogs or microblogs (i.e. Twitter); personal websites or web pages; listservs or mailing lists; audio, photo or video sharing websites (i.e. YouTube, Google Video, Flickr, and Picasa); virtual worlds (i.e. Second Life); or other user-generated electronic media, whether now in existence or invented in the future. The absence of or lack of explicit reference to a specific site does not limit the application of this policy.

**Use of Technology During Work Hours**

During work hours, employees should only participate in business pertaining to the Association. However, the Association consents to incidental personal use of Association-owned and personal computer systems and telecommunications devices during work hours as defined in the Hours of Work policy. The term incidental as used in this context means infrequent and of limited duration, but what is considered incidental is determined at the sole discretion of the executive director. The only sure way to avoid violating this policy is to refrain from any personal activity during work hours.

Participating in social media games or technology supported games during work hours is strictly prohibited.

**Use of Association-Owned Technology During Work or Nonwork Hours**

The Association’s technology systems (including but not limited to telecommunications devices; computer equipment; software; email, internet browsing, File Transfer Protocol; and networking and intranet systems) are to be used for business purposes in serving the interests of the membership and in the course of normal operations.

**Prohibited Activities**

The display of any kind of sexually explicit image or document on any Association system is prohibited. Sexually explicit material may not be archived, stored, distributed, edited or recorded using the Association’s network of technology resources.

Employees may not engage in any activity that violates the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

Employees may not engage in any activity that violates the rights to privacy of protected healthcare information or other confidential Association information.

Employees may not engage in any activity to introduce malicious software purposefully into a workstation or network (e.g. viruses, worms, Trojan horses, etc.).

Employees may not circumvent or attempt to avoid the user authentication or security of workstations or accounts. Employees may not access or try to access electronic data for which they are not authorized nor log into an account that they are not authorized to access.

Streaming video and music for personal use are not allowed on Association computers.

When using Association-owned telecommunications devices, employees are prohibited from calling 1-900, 1-976 or other similar “pay per minute” services or making personal long distance calls on office telephones (land lines). In addition directory assistance (411) calls should be kept to a minimum.

Employees may not connect to the Association’s wireless network for Internet access from a personal device.

### Personal Use

The Association consents to the incidental personal use of its computers, Internet connection, email and telecommunications devices (land line phones, cell phones, smart phones, etc.) as long as it does not conflict with the Association’s business use. The term incidental as used in this context means infrequent and of limited duration, but what is considered incidental is determined at the sole discretion of the executive director. The only sure way to avoid violating this policy is to refrain from any personal activity using Association-owned technology systems.

Use of Association-owned systems, including information stored on those systems, to conduct privately owned business activities is not authorized and is strictly forbidden.

Any use of the Internet or Municipal Association Intranet for conducting job searches; forwarding chain emails; soliciting or proselytizing for commercial ventures, religious or personal causes, or outside organizations is strictly prohibited.

**Use of Municipal Association Email Addresses**

Employees must not use Municipal Association email addresses to create or manage personal accounts (i.e. shopping websites, personal bank accounts, social media accounts). Municipal Association email addresses for professional-based social media accounts such as LinkedIn may be allowed with the approval of the employee’s supervisor.

**Privacy of Communications**

Employee communications, both business and personal, on the Association’s computer and telecommunications systems are not private. Users should be aware that the data they create on the Association’s systems is the property of the Association and usually can be recovered even though deleted by the user.

### Monitoring

### The Association reserves the right to monitor all employee usage of Association-owned technology systems to ensure proper working order, appropriate use by employees and the security of the Association’s data. The Association’s management reserves the right to access and inspect any or all user files, for any purpose, including but not limited to, archived material of present and former employees without the user’s consent.

### Software and Applications

All software and applications on Association systems are owned or licensed by the Association. No Association-owned or licensed software or applications may be copied, deleted, distributed or used on any systems other than those owned by the Association without notification of and written consent from the IT manager. No software or applications may be downloaded, installed, distributed from or copied to Association systems without the approval of the IT manager.

**Remote Access**

When accessing the Association’s systems remotely using personal devices, employees must follow the security guidelines published on the MASC Intranet under the resource center tab in the technology section. Remote access is restricted to business use.

Nonexempt staff (as defined by the Fair Labor Standards Act) may occasionally need to access the Association’s technology systems remotely when staffing the receptionist desk or working at an off-site work function. The Association strongly discourages nonexempt staff from working remotely at any other time using the Association’s technology systems unless approved by the employee’s supervisor. All work, as defined in the hours of work policy, whether in or out of the office, must be recorded on time sheets. This includes time worked while connected remotely to the Association’s technology systems. As stated in the overtime policy, nonexempt employees must receive authorization by their supervisor before working over 40 hours in a work week. The Association’s technology systems may be checked periodically to assess proper use by employees.

**Security**

Although the IT Department does everything possible to protect the Association’s systems and the confidentiality and integrity of the Association’s information stored on its computer systems, employees are responsible for all activities that originate from their computer accounts, systems or telecommunications devices and are responsible for protecting data and information stored on the Association’s electronic equipment from unauthorized access and disclosure. In addition to sensitive information such as social security and credit card numbers, the Association processes data which must remain confidential because of governmental rules and regulations.

Employees are required to lock their computers when not in use and must log off at the end of each work day.

Employees must not share their technology passwords with anyone other than the IT staff whether by phone, print, in-person, electronically or any other means.

Employees must immediately report loss or theft of any technology device to the IT manager or the executive director.

### Archiving and Backup of Systems

Employees are responsible for ensuring that data is stored in the proper location to allow centralized data backups. No Association data should be stored on the employee’s local drive. An employee with questions about the proper location and storage of Association data should contact his supervisor or manager.

**Municipal Association Social Media Sites**

Facebook and Twitter are used strategically as part of the Association’s communication and outreach efforts. Only employees designated by the executive director are authorized to post on the Association’s social media sites.