Guidelines for Section Laptop Computer

Purpose:
To guideline is intended to ensure the section laptop computer is appropriately used and maintained by responsible section members. It is not intended to be overly restrictive, but to help protect the computer and its content from loss, damage, or unauthorized use.

Control Responsibility:
The Section Chairperson will be responsible for assignment of the section laptop computer to a specific individual who is a member of the Section 205 Executive Committee. This is to ensure its care and use is appropriately controlled to prevent loss or damage to either the computer or its content. A System Administrator will be appointed to oversee the technical integrity of the computer.

Intended Use:
The computer must be used for ASQ-related use only. Any personal use must be approved by the Section Chairperson or the System Administrator.

The computer is considered the "Master Database" for ASQ Section 205. Data files will be considered the formal source of information related to section procedures, historical records, and reference information. The source of data files and last date of revision shall be maintained shall be defined.

> **NOTE:** It must be recognized that data files may originate from other computer systems. If there is any question as to the current revision level of a file, the originator should be contacted for verification or obtain the latest version.

In addition to maintaining important operational information (email communications, correspondence, letters, procedures, financial reports, section management plan (SMP) records, data, contacts lists, reference documentation and historical records, the computer is intended to be used in conjunction with the section's projector to support technical presentations at dinner meeting, conferences and other Section 205 events.

Security:
The content of the computer storage is expected to contain only Non-Confidential information and accessible to any authorized ASQ user. Therefore, entry onto the computer is NOT password protected.

> **NOTE:** At the current time, computer password protection is NOT considered necessary, since no confidential Information is being stored in the system. Computer entry passwords must NOT be activated unless authorized by the System Administrator and appropriate access controls are put in place.

The computer may be used for email and Internet searches related to ASQ business. However, the susceptibility to of the computer for viruses and unauthorized access must be kept in mind by the Assigned User(s). An active security program must be maintained at all times.

Additional social media programs such as Facebook, Twitter, Linkin, etc. shall be installed without the approval of the Section Chairperson and the System Administrator.

System Administrator Responsibilities:
The System Administrator is responsible for ensuring the technical integrity of the computer by overseeing the Windows 10 operating system level, the application programs installed, and the internet security software. Other that routine updates; no additions, deletions or changes are to be made without the knowledge of the System Administrator. The System Administrator will be responsible for resolving any warranty or repair issues.

The System Administrator will recommend the filing structure to be used on the computer.

Assigned User Responsibilities:
The Assigned User shall protect the computer from loss or damage at all times. Proper protection and transportation methods shall be implemented to protect against excessive shock, vibration, temperature, humidity or environmental factors that could damage the computer or its contents.

The Assigned User shall ensure "important data files" are backed up on a suitable storage device at least monthly. Any "critical files" shall be backed up each time they are revised. A "critical files" is considered one that, its loss or damage, would prevent the effective operation of Section 205.

> Note: Attachments to emails will be considered "important files" if they are saved in an appropriate file folder on the computer. Subsequent revisions to the attachment will be immediately filed by the Assigned User to override the previous version. This practice should help ensure the latest information is available. Originators of data files may also provide updated files by way of a memory flash drive. In those cases, the file Originator will work with the Assigned User to update files on the computer. The frequency of such updates shall be agreed upon between the Originator and the Assigned User.