AOLS STAFF INFORMATION AND INFORMATION TECHNOLOGY USAGE POLICY

Information and Information technology assets are critical to the success of the Association of Ontario Land Surveyors (AOLS) and represent a significant investment. As such they need to be protected and used properly. The data created during your employment along with e-mail, computer, Internet and voice-mail systems are AOLS's property. The AOLS also licenses a variety of software that is for the use of the AOLS staff and license agreements need to be adhered to.

An employee's communications and use of the AOLS e-mail, computer, Internet and voicemail systems will be held to the same standard as all other business communications, including compliance with the Company's discrimination and harassment policies. Employees are expected to use good judgment in their use of AOLS' system. Transmission of sexually explicit pictures, jokes, or material is strictly prohibited as is the visiting of inappropriate websites. Management should be notified of unsolicited, offensive materials received by any employee on any of these systems.

Furthermore, an employee's consent and compliance with e-mail, computer, Internet and voicemail policies is a term and condition of employment. Failure to abide by these rules or to consent to any interception, monitoring, copying, reviewing and downloading of any communications or files is grounds for discipline, up to and including discharge.

<u>Overall Security</u>

The Executive Director will ensure that adequate firewalls, virus protection and backup procedures are in place.

The AOLS will not provide administrative privileges to its employees. Administrative privileges will be reserved for the AOLS IT service provider and one separate account that the Executive Director will possess and keep safe for use in the event of problems with the service provider. Software should only be loaded by the AOLS IT service provider and anyone requesting software to be loaded needs to ensure that appropriate license or ownership provisions are adhered to.

<u>Personal Use</u>

Personal use by an employee is prohibited while the employee is on office hours. AOLS may intercept, monitor, copy, review and download any communications or files employees create or maintain on these systems.

All electronic communication services and devices provided by the AOLS must not be used for games, harassment, or offensive messages. Use of such services and devices by an employee on working time for solicitation and other non-business-related reasons is not acceptable.

Employees of the AOLS shall not consider things like computer discs, computer programs, computer journal entries, e-mail, voicemail or any other electronic communication within or from the AOLS network to be the Employees' private property.

Because of the danger of computer viruses, employees may not use any personal removable media or unauthorized network device on computers and other such equipment without the consent of IT Support Management.

Internet/E-mail

When using the Internet, do not send materials of a sensitive or confidential nature unless the information is properly coded to prevent interception by third parties.

Access Protection

Passwords for accessing the AOLS' computer resources (the network login) must not be shared with any other person, including a supervisor or manager. Passwords shall be sufficiently complexity as to avoid guessing or copying of passwords. Password changes may be required by the network server every 6 months. Password protecting documents or spreadsheets may only be done with management approval.

Employees must lock or log-out of their Computers before leaving their workstation unattended to prevent the risk of desktop, log-in credentials, and residing data being compromised.

Intellectual Property

AOLS staff shall not copy or distribute any information or software that is subject to copyright and/or license protection.

Data Storage

Data will be stored and managed in accordance with provided file structures and record retention schedules, if they exist.

Information on individual PCs is backed up, however, critical documents and spreadsheets must not be stored on individual PC hard drives*. (Note: There may be some instances in which storing information locally is required by a software package. Special procedures will be taken in these cases.)* Each person has a special, secure area on the network file server, designated as their **(U:) drive** or Users directory, where all information not needed by others should be stored. Shared information, which others may need to access, must be stored under shared areas of the network, such as the **(P:)** drive or Public directory on the network file server.

External/Remote Computer Usage

When away from the office, laptops and other AOLS technology must be kept in a secure location. Try to avoid leaving unattended equipment in a car.

AOLS staff shall use VPN software when sending or receiving any confidential or sensitive data on open Wi-fi networks.