John Readings Computer Use Policy and Procedures

Policy

John Readings is committed to ensuring that staff use computer technology in a manner that promotes a safe work environment. Individual workspaces, furniture and equipment must be adjusted to suit the ergonomic requirements of the user.

All staff members are expected to be able to use a variety of software programs in the course of their daily duties; manage computer data proficiently; and maintain computer equipment in good order and condition.

Procedures

Hardware

* Do not eat or drink near your computer or laptop. Spills can permanently damage the equipment,
* Develop a routine to maintain your computer equipment. The keyboard, monitor and mouse should be cleaned regularly. Before cleaning, make sure the computer is turned off,
* Store any user manuals for your computer in a place where they can easily be accessed for reference,
* Report any suspected hardware problems to the IT Manager,
* Portable devices, such as laptops, smartphones (e.g. iPhones) and tablets (e.g. iPads) are especially vulnerable to physical damage, loss or theft,
* Avoid dropping or knocking about mobile devices, ensuring they are kept secure in protective casing where required,
* Carry and store your laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. An ordinary-looking briefcase is less likely to attract thieves than an obvious laptop bag,
* Keep your laptop, tablet or smartphone in your possession and within sight whenever possible, just as if it were your wallet or handbag. Lock them away out of sight when not in use, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office and in a hotel,
* Never leave a mobile device visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the boot or glovebox. The physical security of any company-owned mobile IT devices in your possession is your personal responsibility. Please take all reasonable precautions to keep these devices safe and secure.

Software programs

* Only registered software programs may be used. Do not download, install or use unauthorised software programs. Unauthorised software could introduce serious security vulnerabilities into the network as well as affecting the working of your computer. Software packages that permit the computer to be ‘remote controlled’ and ‘hacking tools’ are explicitly forbidden on John Readings equipment unless they have been explicitly pre-authorised by management for legitimate work purposes.
* Be careful about software licences. Most software, unless it is specifically identified as ‘freeware’ or ‘public domain software’, may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and the company into disrepute by breaking the law.
* Authorised programs installed on each workstation are as follows:
	+ Operating system – Microsoft Windows,
	+ Antivirus software – Symantec Antivirus,
	+ Office software suite – Microsoft Office Professional,
	+ Internet browser – Mozilla Firefox,
	+ Email software – Microsoft Outlook Express,
	+ File compression/decompression software – WinZip,
	+ PDF reader – Adobe Acrobat Reader.
* Selected workstations also have specialised software relevant to job requirements. These include:
	+ Accounting software – MYOB,
	+ Design and publishing software – Adobe Creative Suite,
	+ Customer relationship management (CRM) software – Act!
* If your computer notifies you that an update is required, follow the instructions. and update the system or software.
	+ These updates could relate to security flaws and it is imperative all software is secure,
	+ Some software updates will try to get the user to install additional tools or add-ons for sister companies. Ensure to deselect all added options and only install the required update.
* Use the software’s online Help files if you require assistance with the program.
* Report any software problems immediately to the IT Manager.

Virus protection

* The server and all computers have antivirus software installed and they are automatically updated at least twice per week. Staff members are not to tamper with the antivirus or update settings on their computer.
* Viruses are a major threat to your organisation and laptops are particularly vulnerable if their antivirus software is not kept up-to-date. Ensure your laptop virus software has been set to automatically update.
* Staff are requested to exercise caution at all times:
	+ Email attachments are now the number one source of computer viruses. Do not open email attachments that are from an unknown source.
	+ Do not copy/open files from an external source (USB flash drive, external hard drive, CD/DVD-ROMs, etc.) until they have been scanned by the antivirus software. This should be automated by your computer; if not, notify the IT Manager.
* Read carefully any emails or memos from the IT Manager regarding virus risks.
* Report any suspected virus immediately to the IT Manager.
* Do not forward any files or upload data onto the network if you suspect your computer might be infected.

File management

* Create a personal subfolder within the server (using your name as the subfolder name) to hold your day-to-day working files.
	+ Do not store company data on your computer unless absolutely necessary. Company data should be stored in the appropriate server drive. Unlike the servers which are backed up automatically, data on your own computer is not backed up and your work may be lost if you experience a system crash.
	+ If you use a laptop and require access to files offsite, you will be set up with offline files allowing remote access to server files away from the office.
* ‘Move’ completed files to the appropriate folder in your department.
* Filenames:
	+ Speak to your Manager regarding the file naming conventions used in your Department,
	+ For ease of operator identification, add your initials to the end of each filename. For example, JulyConf-mq.doc (document about July Conference-keyed in by Mary Quinlan).
* Back-ups:
	+ Back-up copies of all electronic files on the server are made twice week.
	+ If you spend an extended time away from the office network using a laptop, it is your responsibility to ensure local copies of company files are backed up.