Acceptable IT Usage Policy

This Acceptable IT Usage Policy covers the security and use of all EC Training Pty Ltd T/as Work Skills (and all other associated entities); (herein referred to as 'The Company') information and IT equipment.

It also includes and applies to the use of email, internet, voice, Mobile/Wi-Fi Internet Devices such as 3G/4G/ETC dongles and routers and mobile IT equipment. This policy applies to all employees, contractors, agents; and users of proprietary products such as WOLAS and PleaseSign (hereafter referred to as 'individuals or Users'). This policy applies to all information, in whatever form, relating to The Company business activities nationally and worldwide, and to all information handled by The Company relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by The Company or on its behalf.

Computer Access Control – Individual's Access to The Company IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on The Company IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any The Company IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access The Company IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to The Company IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Company authorised device to The Company network or IT systems.
- Store Company data on any non-authorised Company equipment.
- Give or transfer The Company data or software to any person or organisation outside The Company without the written authority of a Company Director. Managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of The Company internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to The Company in any way, not in breach of any term and condition of employment and does not place the individual or The Company in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

• Use the internet or email for the purposes of harassment or abuse.
• Use profanity, obscenities, or derogatory remarks in communications.
• Access, download, send or receive any data (including images), which The Company considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
• Use the internet or email to make personal gains or conduct a personal business.
• Use the internet or email to gamble.
• Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
• Place any information on the Internet that relates to The Company alter any information about it, or express any opinion about The Company, unless they are specifically authorised to do this.
• Send unprotected sensitive or confidential information externally.
• Forward the Company email to personal (non- The Company) email accounts (for example a personal Hotmail account).
• Make official commitments through the internet or email on behalf of The Company unless authorised to do so.
• Download copyrighted material such as (included but not limited to) music media (MP3) files, film and video files without appropriate written approval from a Company Director.
• In any way infringe any copyright, database rights, trademarks or other intellectual property.
• Download any software from the internet without prior approval of the IT Department.
• Connect the Company devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy In order to reduce the risk of unauthorised access or loss of information, The Company enforces a clear desk and screen policy as follows:

• Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

• Care must be taken to not leave confidential material on printers or photocopiers.

• All business-related printed matter must be disposed of using waste bins or shredded.

Working Off-site It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

• Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car and where possible not left overnight in a car.

• Laptops must be carried as hand luggage when travelling. All notebooks are to be protected by a sleeve or bag.

• Information should be protected against loss or compromise when working remotely (for example at home or in public places).

• Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password and/or a PIN. Mobile Storage Devices Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Software Employees must use only software that is authorised by The Company on The Company computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on The Company computers must be approved and installed by the The Company IT department.

Individuals must not:

• Store personal files such as music, video, photographs or games on The Company IT equipment.
• Antivirus protection The Company IT department has implemented (NOD32), an automated virus detection application is to have been installed on all The Company Computers. Users of The Company supplied Computer Hardware (such as notebooks, desktop computers and the like) are responsible that the antivirus software NOD32 is currently installed on any Company device they use and updated and working as designed at all times.

Individuals must not:

• Remove or disable anti-virus software.
• Attempt to remove virus-infected files or clean up an infection.

Telephony (Voice) Phone System Equipment Conditions of Use.

Use of The Company telephone system is intended for business use. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

- Use The Company voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon cancellation /completion of training program or Termination of Contract is that ALL The Company equipment and data, software and the like, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, Wi-Fi internet dongles and devices must be returned to The Company at cancellation/completion of training program or termination of employment or contract. All The Company data or intellectual property developed or gained during the period of employment remains the property of The Company and must not be retained beyond termination or reused for any other purpose**.**

IT system logging software is installed and operational on all Company Devices and any Private Devices that access The Company Network for the purpose of managing and monitoring usage.

The Company will where appropriate, investigate where reasonable suspicion exists of a breach of this or any other policy. The Company retains the right as far as is reasonably allowed by law to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse

- It is your responsibility to report suspected breaches of security policy without delay to your manager. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with The Company policies.