Policy – IT use and Internet

Purpose & Scope

The Academy of Entrepreneurs is committed to protecting the organisation from the risks associated with the use of technology. This policy covers the obligations of the user and accountabilities for general use, email, Slack, G Suite, Dropbox, iCloud, TRUSS and internet usage, portable equipment and storage devices, surveillance and monitoring and malicious software protection. It explains the requirement for all employees to safeguard all electronic information and IT systems that are within their care.

It is all employees' responsibility to adhere to this policy and breaches of this policy may result in disciplinary action. The CEO / IT Department is responsible for administering this policy.

Employees are expected to raise any concerns to management, about behaviour, in accordance with the process outlined within this policy.

Definitions

IT – Information Technology

User ID – Employee User Identification utilised to access and use IT systems

Social Media – all online media which allow user participation and interaction including (but not limited to):

- social networking sites, e.g. Facebook, MySpace, Instagram, LinkedIn, Pinterest, WeChat, Whatsapp, Pinterest
- video and photo sharing websites, e.g. Flickr, YouTube, Instagram
- micro-blogging and activity stream sites, e.g. Twitter, Yammer, SnapChat
- blogs and blogging platforms, e.g. WordPress, Blogger, Tumblr, Medium
- forums and discussion boards, e.g. Trove Forum, Yahoo! Groups, Google Groups, Facebook Group, MeetUp
- online encyclopaedias, e.g. Wikipedia
- any other websites that allow individual users or companies to use simple publishing tools, e.g. wikis

Company IT Equipment - technology, both hardware and software that is owned by the Academy of Entrepreneurs provided for the purposes of undertaking the position.

Portable Equipment - Portable equipment is deemed to be laptops, computers, tablets, smartphones, or other technology which provides access to organisational data. This also includes all relevant computer storage devices such as CDs, USBs, detachable hard-drives, and memory cards.

Personal IT Equipment – equipment owned by the employee, an example being personal laptop or smartphone.

Public IT Equipment – equipment provided for public/customer use an example being utilising public internet connections such as logging on at the airport lounge.

Content

Users must:

- maintain the security of their IT equipment
- maintain the secrecy of all IT system passwords
- lock or log off their workstation, if they leave it unattended
- log off and/or restart their workstation at the end of each work day or shift
- be accountable for any activity performed under their User ID
- complete any required compliance training
- apply reasonable security practices to protect IT equipment and/or information in their possession from unauthorised physical access, theft, or damage
- report the potential/actual loss or theft of IT equipment as soon as possible
- report any suspicious computer activity to CEO / IT department
- undertake any software updates as directed by the Company in a timely manner

Users must not

- share or disclose their user identity and/or password with anyone else
- install unauthorised software or hardware
- bypass, circumvent or modify IT Security controls or programs

- use another person's User ID
- remove, transmit or copy confidential or personal information from the organisation without authority
- download material or install screensavers which may be considered sexually explicit, pornographic, obscene, harassing, defamatory, politically motivated, religiously motivated, portray extreme violence or which are otherwise unlawful or could be considered offensive or inflammatory
- deliberately attempt to access 3rd party resources or information unless they have a bona-fide business requirement to do so
- obscure or misrepresent their identity on any organisation resource

Breaches of this Policy

Non-compliance with this policy may result in disciplinary action including termination of employment or termination of contract agreement with the relevant member of the organisation.

IT access may be removed if this policy is breached, if an employee is suspended, dismissed, retrenched or breaks the law, or, if such action is required to protect evidence that may exist within the organisation.

Security

General Use:

- users are required to comply with this policy
- users are able to use IT equipment and resources for reasonable and appropriate personal use
- users are required to use reasonable, responsible and ethical behaviour when using IT equipment and systems
- use may be removed without notice at any time

Information Storage:

- portable storage devices must be used with care at all times and reported immediately, if lost or stolen
- apply reasonable security practices to all portable devices and only store organisation information on these devices on a short term basis; this includes removal of the device when the computer is left unattended and physically securing the device when leaving
- ensure that all the organisation's information is permanently removed and not just deleted prior to disposal

Email Usage

- email is a tool to be used by the business in a responsible, professional and lawful manner
- limited personal use is permitted provided that the use is lawful and as long as this does not interfere with the user's duties or the duties of others, or interfere with the delivery of products or services to clients
- users must refrain from opening email attachments from unknown or questionable sources
- users must not send or forward chain email messages
- users must not harvest or otherwise collect information about others, including email addresses, without their consent
- users must not mislead others as to the identity or origin of an email message
- users must not send emails containing credit card numbers
- emails should not publish, distribute or display information that may cause harm to the organisation
- users must not knowingly send, store or upload material containing viruses, worms, trojans or other malicious programs
- users must not use IT resources to send or store any messages and/or materials that are sexually pornographic, obscene, harassing, defamatory, politically motivated, religiously motivated, portray extreme violence or which are otherwise unlawful
- emails must not be used to undertake, share or store material that may be construed as sexual harassment, workplace harassment or bullying, defamation, breach of confidence and/or copyright infringement

Surveillance and Monitoring

The organisation may use content-analysis and filtering technologies to perform computer monitoring and surveillance. The purpose of this is to protect the organisation and its users, ensure their IT equipment and resources are being used appropriately and maintain the effectiveness of the IT environment.

This may include reviewing emails, files and documents that are received, sent, stored and accessed and the content of these files. This may also include reviewing what internet material has been accessed, downloaded or searched.

The organisation reserves the right to inspect, record, use and/or disclose any information communicated or stored within the organisation's IT environment in the course of investigations as part of normal business

practice or for any other lawful purpose it deems fit. The organisation may also report to the law enforcement authorities any suspected illegal activities.

Internet Usage

The Internet is an important tool for use in business however, users are expected to utilise the tool in a responsible and lawful manner and access should be primarily for business use. Users can access the internet for limited personal use provided it is lawful and this does not interfere with the user's duties or the duties of others, or interfere with the delivery of products or services to customers.

Users are not permitted to:

- access or view, download or store websites or materials which may be considered sexually explicit, pornographic, obscene, harassing, defamatory, politically motivated, religiously motivated, portray extreme violence or which are otherwise unlawful
- access and use web-based emails unless specifically authorised
- download copyrighted material without authorisation
- publish, blog, distribute or display information on the organisation without authorisation, or which may cause damage to the organisation
- store or transmit large files
- use the features and facilities of the Internet or external websites for unauthorised disclosure of confidential information or processes of the organisation
- send, store or upload material containing viruses, worms, trojans or other malicious programs
- post any blog posts that contain derogatory, religious, discriminatory, disparaging, defamatory or harassing comments

Social Media

Limited personal use of approved Social Media sites during work hours is permitted, if the use is lawful and does not interfere with the user's duties or the duties of others, or interfere with the delivery of products or services to customers.

The organisation reserves the right to monitor the use of social media sites when using the organisation's IT equipment. It also reserves the right to withdraw employees', independent contractors', temporary or casual workers' access, through the organisation's IT system, at any time. The organisation will

also determine the Social Media sites that are accessible through their IT environment.

Any communications using Social Media for representing the organisation is prohibited except for those users authorised to do so.

Please refer to the Social Media Policy for guidelines as to social media requirements.

Personal IT Equipment

The Academy of Entrepreneurs allows the use of this IT equipment to perform work activities for the organisation; however, the user must ensure that the confidentiality, integrity and availability of all of the organisation's information are maintained. There is no Confidential or Personal Information to be stored on the Personal IT Equipment without authority from the organisation. The user should ensure that adequate Malicious Software protection and Firewall Protection is installed and operating. All organisation information must be permanently removed when the information is no longer required, the user leaves the organisation, it is requested by the organisation or the equipment is being given to someone else for any purpose.

Public IT Equipment

The organisation permits the use of public equipment through an approved network connection; however no confidential or personal information should be accessed or stored due to the increased risks associated with this type of access.

Approvals & review

Policy review date:	30/12/2017
Policy approved by title:	Academy of Entrepreneurs Pty Ltd
Policy approved by signature: