NUMBER	:	POL006_17	PAGES	:	8
VERSION	:	V1.0	CREATED	:	01/08/2017
			LAST MODIFIED	:	01/08/2017
			REVISION DATE	:	01/08/2018

DOCUMENTS :

REFERENCES :
SGAE Children & Vulnerable People's Policy
National Framework for Protecting Australia's Children 2009-2020
Records Management
Privacy
Legislative Compliance
Confidentiality & Non-Disclosure
Copyright & Intellectual Property
Risk Management
Code of Conduct Employee
Student Code of Conduct
VET Quality Framework
Standards for Registered Training Organisations (RTOs) 2015 Cwlth.
National Vocational Education and Training Regulator Act 2011

AUTHORISED : 
EXECUTIVE OFFICER

DATE : 11/07/2017

CONTENT

PURPOSE

The purpose of this policy to clearly define the scope and guidelines within which the employees and students of Southern Grampians Adult Education Inc are permitted to utilise IT, Internet and email facilities.

POLICY

It is the policy of SGAE to provide reasonable freedom for employees to access information, develop knowledge and communicate with business related colleagues and stakeholders.

IT, internet and email facilities are not provided by SGAE for private use or for the personal business use of employees or other stakeholders.

SGAE provides Internet facilities for students for the specific purpose of research and study support. Internet facilities are not provided by SGAE for personal/private or business use of students.

The following preventative measures are in place:

- For the protection of minor children SGAE engages, all social media is blocked from access by all users. Parental locks and restricted sites are in place that prevent the access of inappropriate and/or dangerous sites for children.
- The risk management strategy for reducing the potential for virus, Trojan and other infections of the SGAE IT system that may result in serious financial, privacy and loss of business repercussions includes:
  - all social media is blocked from access by all users including staff;
  - a standalone laptop which is not connected to SGAE's system is to be used for the updating of SGAE's social media;
  - SGAE business emails are not to be used for personal email;
  - Internet access is restricted to use for business and student support purposes only. Internet access is not provided for personal use;
  - Any external drives including USBs that have been used outside of the SGAE system must be scanned before use in the SGAE system;
  - Software of any type is not to be downloaded by anyone without the express permission of the SGAE IT Technician.

DEFINITIONS

App or Application	:	Most commonly a small computer software or program that can be downloaded and installed all at once.
Minor Children/Students	:	Students under the age of 18 years
SGAE's system	:	For the purpose of this policy/procedure this means all of SGAE's internet technology including internet access,

		email, software, computers, printers, mobile phones and all other allied equipment and applications.
Social Media	:	Computer-mediated tools that allow people to create, share, or exchange information, career interests, ideas, and pictures/videos in virtual communities and networks. e.g. Facebook, Pinterest, Instagram, Twitter
Software	:	Set of machine-readable instructions that directs a computer's processor to perform specific operations. Computer software is non-tangible, contrasted with computer hardware, which is the physical component of computers. e.g. Microsoft programs, games, Adobe
Trojan	:	Malicious computer program which is used to hack into a computer by misleading users of its true intent.
Virus	:	Malicious software program that, when executed, replicates itself by modifying other computer programs and inserting its own code. Infected computer programs can include as well, data files, or the "boot" sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

SCOPE

This policy covers:

- the SGAE information and communication technology in its entirety and
- personal information and communication technology used by staff for SGAE business

and includes:

- laptops, desktops and ipads
- landline and mobile phones
- printers and copiers.

ACCESS

All reasonable and safe access of SGAE's information and communication technology will be provided to support students and staff to achieve their potential.

PROCEDURE

Telephone, internet and electronic mail (e-mail) are important communication and research tools for SGAE network users. This document details standards for the secure use of these facilities.

USE OF PERSONAL EXTERNAL EQUIPMENT

Where staff are required to use their personal equipment e.g. for after-hours work or due to working from or working away from SGAE they should:

- ensure that they have adequate firewalls and virus protection on their personal systems (please seek advice from IT Technician if unsure)
- not forward any documents or other items downloaded from the internet.

Should staff require assistance in protecting their personal devices please speak with the IT Technician.

Libel

Legislation provides all parties associated with an email with an entitlement to view any information contained in the email which is about them. If the information is incorrect they are entitled to have it corrected. Parties may include the writer, all recipients and any individuals or entities named in the e-mail.

This means that under the law of libel emails constitute a 'publication' and both SGAE and the author(s) of the email(s) could be sued for libel.

Privacy

All personal or financial information collected or sent via the Internet fall under the Privacy Act.

All information collected via the internet must be collected and stored within the policies and guidelines of SGAE Records Management, Privacy Policy and the Privacy Act 1988.

SGAE reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes.

SGAE reserves the right to demand that encryption keys and passwords, where used, be made available so that it is able to fulfil its right of access to a user's e-mail messages in such circumstances.

SGAE requires that passwords and encryption information is updated to the Executive Officer through the Executive Assistant as soon as created or changed.

Confidentiality

SGAE's Confidentiality & Non-Disclosure and Copyright & Intellectual Property Policies apply to all electronic materials including email.

All files stored electronically are the property of SGAE and may only be transmitted or used specifically for SGAE business purposes. Breach of this policy will result in disciplinary action and may result in litigation against the offender and any third parties involved.

Copyright

The use of the SGAE Internet Connection to download or distribute copyright material is strictly prohibited.

Automatic 'copyright' applies to all emails and as such all e-mail messages sent or received by a user via SGAE facilities are copyrighted and thereby owned by SGAE.

When posting information to a public list/site copyright is retained, however, the message may be archived and forwarded to other lists/sites and/or quoted by others.

Users should keep in mind that all e-mail or internet communication is neither private nor totally secure unless encrypted. Care should be taken before transmitting confidential information.

Other Users' Communications

SGAE users should not at any time monitor or intercept or browse other user's communications unless specifically authorised to do so by the Executive Officer.

Downloads

Software of any type, applications or files are not to be downloaded from the Internet without the express permission of the IT Technician after they have deemed them safe. The files and/or software and/or applications may not be compatible with SGAE systems, may be protected by copyright restrictions and/or contain viruses, Trojans or other damaging programs.

Personal Use

Access to the Internet is provided for SGAE business related purposes for employees and for study and research purposes for students. The facility must not be used for personal use.

Personal and private commercial use of SGAE's email, which is not connected to or approved by SGAE, is strictly prohibited and will result in disciplinary action.

Staff are not permitted to save personal correspondence or documents on SGAE's systems.

Saving to Local Drive C

Backup systems do not backup the C or local drive of PCs or laptops.

Nothing is to be saved to the C or local drive of any SGAE PC or laptop.

Social Media

All Social Media sites are blocked on SGAE's system.

A dedicated stand-alone Laptop is available to the IT Technician and the Executive Assistant to update SGAE's social media content.

Prohibited Sites

SGAE will place controls and blocks on as many prohibited sites as is reasonably possible.

Accessing sites containing pornography or other offensive material or the forwarding of pornographic or other offensive materials including jokes, and other publications is prohibited and are grounds for dismissal or expulsion.

Scanning & Hacki*n*g

Users must not use the SGAE Internet connection to scan or attack other individuals or devices or organisations. The use of port scanners or other hacking tools is strictly prohibited and will result in dismissal.

Only devices approved and supplied by SGAE are permitted to be connected to SGAE infrastructure.

Content

Users must not send messages or use language that is likely to be considered abusive, offensive or inflammatory by the recipient(s) or others who may have access to the communication.

Email content is to be accurate, factual and objective. Users should avoid subjective opinions about individuals or other organisations.

Users must not use a false identity in e-mails.

Users must not create or forward jokes, advertisements, chain letters and/or any unsolicited e-mails e.g. SPAM.

Infection Control

All users should be cautious when opening e-mails and attachments from unknown sources as they may be infected with viruses. If in doubt contact the IT Technician **before** opening the email and/or attachment.

Data Protection

When leaving their desks unattended for any period of time all users, staff and students, are to protect any data displayed on their monitor by initiating the windows  and L together. This will lock their screen.

Excepting for notifying the Executive Officer through the Executive Assistant of a change or new log on and/or password, these should not be shared with other individuals or entities.

Monitoring and Auditing

Users should be aware that e-mails may be subject to monitoring and auditing by SGAE to ensure that they meet the requirements of this policy. This applies to message content, attachments, addressees and to personal e-mails.

All email traffic is to be archived periodically in the designated archive folder or filed in appropriate folders on SGAE hard drive.

Emails must not be deleted when an employee leaves the SGAE.

Note: Deleted emails can be retrieved by specialist IT personnel.

RESPONSIBILITIES

All Stakeholders

It is the responsibility of all users to adhere to this policy at all times.

All security incidents involving internet/email must be reported to the Executive Officer and IT Technician immediately.

IT Technician

It is the responsibility of the IT Technician to:

- ensure that SGAE IT security is kept up to date at all times
- conduct spot checks of all ITC systems
- develop and manage the ITC maintenance plan.