STATEWIDE GROUP TRAINING (SA) INC

INFORMATION TECHNOLOGY POLICY

PURPOSE:
Statewide Group Training (SA) Inc (SGT) provides information technology (IT) facilities, equipment and software for employees to use in accordance with the performance of their specific duties and to enable SGT to operate in the most efficient and effective manner.

SCOPE:

This policy applies to:

- Board Members
- All staff, including: Managers, Field Officers, Administrative Officers; full time, part time, casual, temporary or permanent staff; apprentices and trainees, contractors, sub contractors, and work experience personnel.
- how SGT provides services to clients and how it interacts with other members of the public.
- on site, off site or after hours work; work related social functions; conferences – wherever and whenever staff may be as a result of their SGT duties

POLICY:

In order to ensure that both SGT and its employees are protected from:

- Illegal and/or unauthorised access or use of the IT systems and software;
- Infiltration by spyware and infestation by virus, whether from internal or external sources;
- Breaches of confidentiality and/or loss of intellectual property;
- Corruption and/or loss of data; and
- Legal liability arising from breaches of discrimination and other laws,
-

The acceptable standard of behaviour and usage by all employees in relation to the IT systems, equipment and software is outlined in the Information Technology Procedure.

For the purposes of this Information Technology Policy, "IT equipment" includes, servers, computers, laptops, printers, scanners, copiers, telephones, mobile phones, facsimile machines, mass storage devices, network hardware and cables, digital cameras, data projectors and all other electronic devices, along with any equipment, software and systems required for these devices.

Breaches of this Information Technology Policy will result in the employee being subject to disciplinary action, and in serious cases, termination of their employment contract.

Information Protection/Confidentiality

Any confidential documents or computer outputs that are no longer required should be disposed of in a secure manner by using a security bin or shredder and in line with SGT's Confidentiality Policy.

All data handled on IT equipment must be stored on file servers that are backed up on a regular basis, that is, at least weekly. Discs, USB drives, external hard drives and other mass storage devices must be stored in a secure place and be clearly labelled.

Data stored on IT equipment must be deleted when no longer required by an authorised user.

Passwords must not be recorded or stored in any accessible form and should not be revealed to any person that allows unauthorised access.

INFORMATION TECHNOLOGY POLICY

The unauthorised provision, access or use of confidential, personal or sensitive information, as defined by and in accordance with SGT's Privacy Policy, is strictly prohibited.

Employees of SGT are, without express authority, prohibited from accessing any computer or IT system, whether owned by SGT or any other organisation.

Use of Computer Equipment

All computer equipment must be located in physically secured areas. IT equipment, such as laptops and mobile phones, must never be left in an unsecured site, for example, in open view in a car or at a client's premises.

Any changes to user access and installation, re-configuration, relocation or disposal of IT equipment, systems and software can only be authorised by the Information Technology Officer, Finance Manager or the CEO.

Internet and Email Facilities

Internet and email facilities are provided for the purpose of business communication, research and other legitimate business purposes that are related to the position the employee holds.

SGT reserves the right to monitor or audit staff compliance with the Information Technology Policy relating to usage of both internet and email facilities. Detailed logs of every employee's email usage, web browsing and internet activities will be stored by SGT and management has the right to access these logs, including when employee compliance becomes an issue of concern.

Improper usage of the internet or email by an employee may pose a threat to SGT security, the privacy of other employees and also the legal liability of SGT itself and, as a result, any programs, information or files downloaded from the internet or email **must be** scanned for viruses prior to being opened or stored on any computer/equipment on the network.

Electronic messages are formal business communication and have the same legal status as letter, memos and other printed communication. Both hard copies and electronically stored copies of email communication are subject to the laws of discovery, defamation, libel, harassment, copyright and/or privacy.

The following activities are prohibited when using internet or email facilities:

- Sending, receiving, downloading, displaying, printing or otherwise disseminating material that is sexually explicit, obscene, profane, harassing, discriminating, fraudulent, offensive, defamatory or otherwise unlawful;
- The unauthorised transmission of confidential information;
- The playing of games within working hours;
- Creating and/or sending unnecessarily large volumes of computer network traffic;
- Transmission of large files such as videos and images should be avoided;
- Forwarding chain emails;
- Using or copying software in violation of license agreements or copyright;
- Violating any State, Federal or International law;
- Excessive use of the internet for personal business or private purposes;
- Engaging in online chat groups or real-time exchange;
- Excessive usage of the email facility for personal communications; and
- Use of SGT credit cards on the internet is not permitted, unless authorised by a manager.

INFORMATION TECHNOLOGY POLICY

Security Violations

An IT security violation occurs when an authorised or unauthorised user deliberately accesses, or attempts to access, computer systems or equipment for personal benefit or gain, or to destroy data in order to disrupt business, or for any other reason. Examples of security violations include:

- Attempting to access a computer system, or function within a system, without the proper authorisation;
- Attempting to access a system or log on with another person's User ID;
- Accessing and/or supplying data to an unauthorised user;
- The unauthorised transmission of confidential information;
- Installing unauthorised software or hardware on SGT's IT equipment;
- Removing IT equipment from SGT premises without proper authorisation;
- Providing your password to another individual so they can gain unauthorised access; and
- Falsifying or updating records and systems without proper authorisation.

Computer viruses

The most common way a virus, or other unauthorised software such as spyware, is introduced into a computer system, if from a file loaded, accessed or executed from an external source, such as a disc, an email or via the internet. Therefore, any media, including software, data and images, brought into SGT using facilities such as discs, or mass storage devices obtained from external parties, must be scanned for viruses prior to being connected to the IT system or downloaded.

Viruses are commonly introduced into the system via email transmissions and attachments. Any virus warning on a system must be reported immediately to the IT Officer in such a way that restricts any further infection of the system. Employees are not permitted to take any action themselves.

Deliberate installation of a virus or virus-infected material on to SGT's IT system is an act of serious and wilful misconduct and will result in the immediate termination of the employee's employment contract and may result in prosecution.

Telephone Systems

SGT telephone systems (including mobile phones) are provided for business-related purposes. In accordance with SGT Telephone Use Policy, the limited and appropriate use of the telephone systems for private purposes is acceptable.

APPROVED: KYM ANDERSON DESIGNATION: CHIEF EXECUTIVE OFFICER

APPROVAL SIGNATURE:  DATE: 27TH MARCH 2023
