Secure Use Policy

Version 1: May 2021
Authors: MJ Barcroft, AK Steven

STUDENT TRAVEL MANAGEMENT SOFTWARE

i-gtm

This document sets out the Secure Use Policy of i-gtm.

No printouts
No document containing personally identifying information of any student, client or member of staff is to be printed out. Should any such document be required to be printed for audit, compliance or any other legitimate reason, it should be treated as being strictly confidential and disposed of by shredding as soon as possible.

No screenshots
No screen grabs containing any personally identifiable information should be taken. Anonymised screenshots necessary for training, troubleshooting or compliance purposes should be treated with care and as confidential.

Log out
All users should log out of i-gtm and any other websites, servers or sensitive digital information repositories whenever these are not in use.

Device updates
All devices must be kept updated by installing security patches and updates as soon as available.

Conceal screen from third parties
Screens should be concealed from the view of third parties, especially when mobile devices are being used outside the office or home environment, for example at the airport. Particular not should be taken of the confidential nature of the screen content and every effort made to prevent this being seen by others.

Confidential data hidden
Confidential data, including internal documents pertaining to the operation of the Company and documents containing personal information, should only be stored on the company's cloud storage drive (Google Drive). Access to this data should be hidden and password protected from any family members or others who may have access to a shared device.

Passwords changed from default
i-gtm and its employees, contractors and subcontractors often work from home using their own equipment. It is incumbent upon all staff to change the default password of all their equipment, including broadband routers, wi-fi extenders and other such equipment used to access i-gtm and other internet-based services necessary in the operation of our business.

Router Firewall active
Any member of staff working from home must ensure that their broadband router has an up-to-date firewall and that it is active.

Passwords, passcode, biometric access
Any devices using a passcode should use a random sequence of numbers. Biometric device access should be enabled where available.

i-gtm staff who have a 1Password licence allocated must use this application to generate and store all passwords.

No member of staff should write down or print out any passwords.

Two-factor authentication (2FA) must be implemented where available.

Secure passwords standards
All passwords must meet recommended security standards: Minimum 8 characters containing a random mix of upper and lower case letters, numbers and special characters. Alternatively the three random words standard can be used.

Use of own devices
The use of own devices by members of staff is acceptable as long as the device is running the most recent version of its operating system and that all software patches and updates are installed.

Hard drives or permanent storage should be encrypted so that if the device is lost or stolen its contents are not capable of being viewed.

Virus protection
Where anti-virus software is available for devices, this should be installed and updated regularly.