General Policy G07 Information Technology Network Usage and E-mail Policy

1. Policy Statement

This Acceptable Usage Policy covers the security and use of all SAE information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment.

This policy applies to all SAE employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to SAE business activities, and to all information handled by SAE relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by SAE or on its behalf.

Where SAE data is referred to in this document, it is referring to any SAE-related electronic information, inclusive of electronic material in a printer state, created or gained whilst in the employment of SAE.

2. Access Control

Access to SAE IT systems is controlled by the use of user ID (otherwise known as username) and passwords. All user IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the SAE IT systems. Where login credentials are created locally, e.g. on a stand-alone (not connected to a domain or centrally managed) computer, those credentials should remain private and a complex password should be applied. A strong and complex password should be a minimum of 8 characters long, including lowercase, uppercase, numbers and symbols.

Individuals must not:

- Allow anyone else to use their user ID and password on any SAE IT system, or use someone else's user ID and password.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Leave their password unprotected, for example writing it down, leaving it easily accessible from others or storing it in plain text.
- Perform any unauthorised changes to SAE IT systems, networks or information.
- Attempt to access data, systems or networks 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-SAE authorised device to the SAE network or IT systems, except where ‘guest’ network provision is available or authorisation from either the campus manager or the systems administrator has been granted.

- Store SAE data on any non-authorised SAE equipment.

- Give or transfer SAE data or software to any person or organisation outside SAE without the authority of SAE.

- Attempt to modify or manipulate any physical or virtual area of the IT infrastructure (i.e. staff or student workstations, systems, servers, network equipment), in order to use the resources outside of their legitimate purpose.

- Store personal files such as music, video, photographs or games on SAE IT equipment.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Be aware of social engineering risks whereby intruders may manipulate employees into bypassing normal security procedures, or facilitating access to sensitive information through elaborate deception. You have a duty to challenge and report any suspicious activity at your business to your line manager.

3. Internet and email Conditions of Use

SAE internet and email provision is intended for business and academic use only. Personal use is permitted where such use does not affect the individual’s work performance, is not detrimental to SAE in any way, is not in breach of any term and condition of employment and does not place the individual or SAE 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 SAE considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

- Access, download, send or receive any data (including images) that supports, promotes or facilitates extremism/terrorism. SAE UK has an obligation under the Prevent Duty to safeguard users of its network against content that might support, promote or facilitate terrorism. Therefore, measures are in place to prevent access to such materials and any attempts to do so will be logged and reviewed in line with SAE's Prevent Policy.

- Use the internet or email to conduct 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 SAE, alter any information about it, or express any opinion about SAE, unless they are specifically authorised to do so.
- Send unprotected sensitive or confidential information externally, for example, student personal data contained in a spreadsheet.
- Forward SAE mail to personal (non-SAE) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of SAE unless authorised to do so.
- In any way infringe any copyright, database rights, trademarks or other intellectual property, for example, through the downloading or sharing of copyright protected media, written works and software.
- Google Drive is not recommended for the storage of sensitive personal data. Student or staff personal information, records or credentials should be stored locally (i.e. in local servers/NAS). If you wish to store sensitive personal data in the cloud, you should firstly ensure full compliance with local data protection laws.

4. Email

Email distribution lists can be requested via the Service Desk but must follow the current standard. Information on naming standards and distribution list protocols can be requested from the IT team.

If an email account is suspected of sending spam, access may be suspended until further notice.

Individual's should not forward on information regarding imminent virus threats even if it looks like it's from a credible source. Often the emails are hoaxes and spread unnecessary panic. If in doubt, contact the Service Desk.

5. Software

Authorised software must be used in accordance with the software supplier's licensing agreements.

All software on SAE computers must be approved by the relevant business unit manager and procured through official SAE procurement methods i.e. the Service Desk.

SAE make use of a software asset monitoring system, which must be installed and not tampered with on every SAE-owned computer. Contact the Service Desk for more information.

6. Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, SAE enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using reasonable security features for example security on shared drives and disk encryption on local drives.
- 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, photocopiers, scanners or in plain sight.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

7. Working Remotely

The following controls must be applied on mobile devices and laptops:

- Equipment and media taken off-site must not be left unattended in public places, for example, not left in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Laptop encryption must be used in line with SAE security policies.
- Smart-phones and tablets must be protected at least by a password/PIN and encryption (standard on iOS devices).

- 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.
- Only SAE authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

8. Viruses and Malware Protection

The IT department can facilitate virus and malware detection software for any business within SAE. All computers, regardless of their operating system, should have antivirus software installed.

9. Telephony (Voice) Equipment Conditions of Use

Use of SAE voice equipment is intended for business use. Individuals must not use SAE voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not use SAE voice facilities for conducting private business or making hoax or threatening calls to anyone.

10. Leaving SAE

All SAE equipment and data must be returned to SAE at the end of employment. Under no circumstances is SAE equipment gifted or sold to the employee when they leave.

All SAE data, including but not limited to student and employee personal data, and intellectual property developed or gained during the period of employment remains the property of SAE and must not be retained beyond termination or reused for any other purpose.

Where any items of equipment have been lost or have suffered excessive damage beyond normal 'wear and tear', and where the item has not been previously reported, SAE reserves the right to deduct a fair and reasonable sum from the employee's final salary payment to cover the replacement or repair of the item.

11. Monitoring and Filtering

All data that is created and stored on SAE computers is the property of SAE. IT system logging may take place where appropriate, and investigations of systems and services will be commenced where reasonable suspicion exists of a breach of this or any other policy (e.g. SAE Prevent Policy). SAE has the right (under certain conditions) 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. Any monitoring will be carried out in accordance with local laws.

It is your responsibility to report suspected breaches of security or data protection without delay to your line management, IT management or the IT Service Desk (service.desk@navitas.com). All policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with SAE disciplinary procedures.

12. Policy History

Last Review:	March 2016
Updated:	November 2016
Policy Author:	Daryll Holland, Head of IT (UK and Europe)
Policy Review Date:	1 December 2017

Policy G07: Appendix A: Student Acceptable Usage Policy

1. Scope

This Acceptable Usage Policy applies to all SAE students and covers the use of all SAE information and IT equipment. It also includes the use of email, internet and voice facilities.

2. Conditions of Use

Students will be expected to use SAE campus resources for the educational purposes for which they are provided. It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Policy. Students must also accept personal responsibility for reporting any misuse of the IT resources to an appropriate member of staff.

Students must not:

- create, send or post any material that is likely to cause offence or needless anxiety to other people or bring SAE into disrepute.
- use campus resources to perform illegal activities.
- perform any action that could stir up hatred against any ethnic, religious or other minority group.
- attempt to access another student or staff members' data, or any other data (electronic or physical) which they do not have the authority to access (including websites such as Facebook).
- share login details (including passwords) with anyone else.
- use the campus' internet access for any online business activities.
- use the SAE network in any way that would disrupt use of the network by others.
- introduce "USB drives" or other portable devices to the network without having them checked for viruses.
- attempt to download, view or share any content that might be considered inappropriate or illegal, for example, pornography or items related to hacking, gambling and terrorism. SAE UK has an obligation under the Prevent Duty to safeguard students against content that might support, promote or facilitate terrorism. Therefore, measures are in place to prevent access to such materials and any attempts to do so will be logged and reviewed in line with SAE's Prevent Policy.
- download and/or install any unapproved software, system utilities or resources from the Internet.
- receive, send or publish material that violates copyright law. The use of file sharing programs is explicitly forbidden.
- attempt to alter, harm or destroy any equipment or work of another user on the SAE network
- attempt to modify or manipulate any physical or virtual IT resources in order to bypass their legitimate use.

Students are required to respect their personal information and the personal information of others. All SAE users and guests must understand that their internet and network use will be monitored to ensure compliance of this policy.

By making use of any campus IT resources, you agree to be bound by the terms and conditions of this policy. Any breach of this policy will be investigated and could result in disciplinary action. SAE may in its sole discretion, i) terminate a user’s right to use IT resources, ii) withdraw or remove any material uploaded by that user in contravention of this policy, iii) where appropriate, disclose information to law enforcement agencies and iv) take any legal action against a user for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.