SAE Institute

G07: Information Technology Network Usage and E-mail Policy

1. Policy Statement

This policy provides for approved, legal and efficient use of E-mail and Internet services at SAE Institute campuses in Europe, in Licenced territory operations and at all SAE campuses offering programmes in collaboration with Middlesex University, and sets out the standards that apply to the use of the Information Technology (IT) network, and computer-based and e-mail communication systems.

2. Purpose

This policy aims to ensure the appropriate and legal use of the SAE IT Network and computer-based and e-mail communication systems. The policy provides specific information about what SAE Institute considers acceptable and unacceptable usage of these services.

3. Scope

This policy applies to all SAE Institute operations in Europe, in Licenced territory operations and at all campuses offering programmes in collaboration or operations with Middlesex University, and is applicable to all users of any IT systems or any computer-based communication systems or communication through the use of any other electronic devices. All staff, students and guest users are required to abide by the provisions of this policy in using any of the systems provided by or at SAE Institute.

This policy applies to all users regardless of location, when the user is utilising SAE equipment (computers, laptops etc) or using SAE systems to communicate (e.g. via email), or connected to the SAE network remotely, or when accessing the SAE network or email IT systems on equipment which does not belong to SAE.

4. Associated Policies and Documents

This policy should be read in conjunction with the following policies and documents:

- G01 Code of Conduct
- G02 Public Information Policy
- G06 Information Privacy Policy.

5. Policy

5.1. Principles

The IT network, computer-based and e-mail communication systems are provided to students in order to facilitate their studies and to allow access to online learning and research material.

The IT network, computer-based and e-mail communication systems are provided to all SAE staff (part time, full time or in any employment or contractual capacity) in order to facilitate their work related activities and outcomes at SAE Institute.

Proper usage of all these systems is provided and encouraged to assist staff and students in their work, and to enhance the deployment of modern and emerging technologies to create greater efficiencies, better use of time at work, improved access to information and research data, and more effective modes of communication.

Such SAE Systems must however be used in accordance with this policy in order to protect SAE, its staff and its students from adverse risk which can arise from improper or non-approved use of these systems. Users should not access any systems or accounts except those for which they have been given formal authorisation.

5.2. Potential Risks

Examples of significant risks which may arise from unacceptable usage include, but may not be limited to:

- Breaches of confidentiality in relation to staff or student data
- Copyright infringement of intellectual property
- Harassment, defamation or slander of individuals
- Introduction of malware, viruses or spyware into the SAE network
- Electronic participation in illegal or criminal activities.

5.3. Unacceptable Usage and Behaviours

The viewing, downloading, listening to, posting or circulation of any material considered inappropriate or offensive is not allowed.

The following specific behaviours are unacceptable, and will be viewed as misconduct which could result in termination of studies or employment:

- use of any electronic means in a way that breaches the provisions of the SAE Code of Conduct (Policy G01);
- visiting internet sites or circulating any message or materials that include obscene, hateful, pornographic, racist, sexist, discriminatory, abusive, or malicious content;
- using the internet or e-mails to send offensive, harassing, defamatory or slanderous material to other users internal or external to SAE Institute;
- using computers to perpetrate any form of fraud, or software, film or music piracy or use of any kind of peer-to-peer or torrent software or structure;
- participation or involvement in any electronic campaign intended to damage or bring disrepute to individuals or organisations;

- downloading commercial software or any copyrighted materials which belong to third parties without appropriate authorisation or licence;
- hacking into unauthorised areas of SAE Institute or other organisations;
- publishing or circulating defamatory or false material about SAE Institute, fellow students or staff on social networking sites, 'blogs' (online journals), 'wikis' or any other form of online publishing format;
- undertaking deliberate activities that waste staff effort or networked resources;
- introducing any form of malicious software into the corporate network;
- usage which in any way infringes the reasonable rights of others members of staff or students;
- use of the network or SAE systems for unauthorised or non-approved personal gain or benefit;
- the use of network mapping software, or packet sniffers on any segment of the SAE network;
- the use of any software or systems in order to circumvent or bypass network security and access control.

5.4. Personal Use

Limited use of SAE systems for personal communications by staff or students is permitted provided that it is strictly kept to a minimum during working hours or formal study times, that it does not interfere with work duties or the normal responsibilities of the staff member or the academic work of the student, that it does not interfere with the normal academic activities or business operations of SAE, and that the usage conforms to the provisions of this policy.

Where a staff member or line manager has reason to believe that a student or staff member is making unreasonable private usage of SAE resources then this permission for personal usage may be withdrawn by the Campus Manager or other responsible senior staff member.

5.5. Monitoring and Control

All internet-related and electronic resources and systems are provided for

study purposes or for work purposes. To ensure both policy and legal compliance SAE Institute maintains the right to monitor and log internet and network traffic, including browsing history, together with the internet sites visited in accordance with local legislation. The specific content of any electronic transactions or communications will not normally be monitored unless there are reasonable grounds to infer improper or illegal use. Any decision to monitor content should be authorised by the Campus Manager or an appropriate senior officer.

All staff email and communications sent or received using IT Systems are stored, and may be accessed after approval by a senior manager if required. Examples of authorised purposes may include:

- to detect unauthorised use of the systems
- to protect systems against malware and exploitation
- to retrieve data in the event of computer failure
- to comply with legal obligation
- to prevent or detect crime
- to investigate a serious complaint.

Such gathered information will normally be stored for at least 1 year, and will not be shared with any parties unless authorised or as demanded by legal obligation.

5.6. Login Obligations

It is the responsibility of each user to ensure that the security and confidentiality of login credentials is maintained, and revealing access passwords to unauthorised persons in any part of SAE operations may incur disciplinary action.

Login and access passwords must be secure and adhere to the password policy:

- that unless otherwise approved, all passwords are required to be 6 characters or more in length, and contain a mix of at least 2 of the following:
  - Upper case characters
  - Lower case characters
  - Numbers
  - Non-alphanumeric characters.

Consecutive strings of characters are not permitted (e.g.: AbcdEfg or 1@345^ are considered weak passwords and are not permitted)

5.7. Internet Usage

5.7.1. Downloading

Software programs, modified applications, music or other creative or electronic content should not be downloaded by students onto any IT systems unless permission has been granted or specific instructions have been issued by the IT department or an appropriate SAE staff member (e.g. administrator, lecturer, or manager).

5.7.2. Use of E-mail

Email is stored, considered to be permanent and a publication in a court of law.

Particular care should be taken with sensitive or confidential information transmission.

The sending of email from any work account makes that person an agent of SAE, and care should be taken that any communication reflects well on SAE Institute.

Special care should be taken when opening attachments to email in case of spreading malware or any virus. Any student or staff member who believes they may have contributed to the spread of a virus or malware should immediately notify the IT officer.

Further advice and guidance on e-mail usage is attached in Appendices A and B.

5.7.3. Websites, Copyright and Social Media

Use of any SAE Websites is subject to the terms of this policy and or any policies contained in the websites.

Staff should ensure that any information placed on SAE websites is correct, complete and current, that it complies with all relevant policies (especially G02 Public Information Policy) and has been approved by the relevant manager.

Staff should ensure that all material posted on websites or social media is copyright free, or that the copyright is owned by SAE, and that relevant permission has been obtained for any copyrighted material.

Further advice and guidance on the use of social media is in Appendix A of Policy G02 on Public Information.

5.8. Workstation and Network Security

Individuals are responsible for ensuring the security of their assigned workstation or laptop, and they must ensure that unauthorised persons do not access them.

All workstations and SAE laptops must have the relevant licensing software installed and running, and staff or students must not install or run any applications that have not been approved by the relevant IT officer or Campus Manager.

Log out of all services and websites should occur when leaving a workstation in order to prevent unauthorised access.

The SAE network should not be used to download, distribute or access illegal, offensive or copyrighted materials unless (in the case of copyright materials) you have been granted permission to do so by the copyright holder.

The use of peer-to-peer file sharing software and direct link download sites (rapidshare) is prohibited an any SAE network.

5.9. Software Use and Installation

Software use is limited by copyright and licensing. Only software installed by the relevant IT officer under authorisation from the Campus Manager and which the user has permission to access should be utilised.

The copying or distribution of software without authorisation is strictly prohibited, and prior permission must be sought and granted before the installation of any software or plugins.

Staff or students working on an SAE laptop should ensure that all software installed on the laptop is fully licensed and conforms to this policy.

5.10. Data Protection

All staff are required to comply with the provisions of Policy G06 on Information Privacy as well as the current related local legislation, and must take all reasonable precautions to ensure that private information relating to staff or students is kept secure from unauthorised access.

6. Breaches and Disciplinary Action

Any breached or non-compliance with this policy will be treated as breaches of the Code of Conduct i.e. as misconduct, and may result in disciplinary proceedings.

7. Version Control

July 2007 policy implemented (Governing Council)

September 2009 policy amendment (Governing Council)

October 2011 policy amendments approved (CEO and Managing Director)

April 2012 policy revisions approved (CEO and Managing Director)

April 2013 Policy revised (approved CEO, and Director of Academic Affairs)

APPENDICES A and B follow.

Appendix A: E-mail Use and Management Guide

1. Managing Emails

Employees and individuals must actively manage their e-mail and adhere to the following guidelines;

a) E-mail etiquette principles as per the E-mail Etiquette Guidelines (Appendix B)
b) Size implications of e-mail.
c) Storing and archiving e-mail.
d) How to deal with unsolicited and/or inappropriate e-mail.

All employees and individuals are required to check their e-mail on a daily basis.

2. Size of E-mail Messages

E-mail use involving large files (eg video files or large photo files) creates congestion on the network and disruption to e-mail services. Employees and individuals should be conscious of the size of the e-mail message they are sending.

Employees and individuals should avoid:

- Sending large attachments to users with a low-speed network connection.
- Sending attachments to large distribution lists.
- Sending, forwarding and/or replying to large distribution lists concerning non-SAE Institute business.

Multimedia attachments should only be sent as an e-mail attachment if required for business reasons, that is, multimedia files are not normally to be sent as part of personal e-mail.

How do I determine the size of an e-mail?

Employees and individuals are able to determine the size of an e-mail within the e-mail client. Briefly, by saving the e-mail/attachment as a draft and Pressing (Apple + I) (or “Get Info”) to get information or selecting properties from the file menu, you can determine the size of an e-mail or attachment.

What is an acceptable e-mail size?

It is important to be mindful of the size of an e-mail when sending a message. This is to ensure that clients are able to access and download any attachments in a timely fashion. The acceptable size, however, depends on the bandwidth of the network link being used by the recipient. Always ensure that you ask the recipient if they have any restrictions regarding the size of attachments they may receive prior to sending it.

It is particularly important to use small messages when sending to distribution lists as these have the potential of putting severe strain on the network.

How do I reduce the size of an e-mail?

It is quite simple to increase the size of an e-mail message unknowingly. Some examples include inserting graphics in auto-signatures, including a background image in a mail message and using graphics within attachments. Where possible and practical employees and individuals should use the following techniques:

- Avoid sending large attachments, particularly to Distribution lists.
- Avoid the use of pictures as the background for messages, or inclusion of a picture in an auto-signature.
- Changing the font attributes (font size, colour, etc.) has little effect on the size of the message and is therefore quite acceptable (but remember some e-mail systems do not handle bolding or italics very well).
- Avoid sending large multimedia files. There may be some instances where this is necessary for valid business reasons but generally this should not be required.
- Do not spread non-work related messages, for example jokes, pictures, video clips and other multi-media files by forwarding them to all your colleagues.
- Avoid sending the same attachment in multiple formats (e.g. publisher and word).
- Convert large attachments to a web format and publish to a suitable web site and then advise your audience of the web address. This is appropriate for information that has to be disseminated to a large audience but can result in a significant delay whilst approval is sought to publish to the web.
- Use a compression tool (e.g. zip, stuffit, Winzip) that both the sender and recipient have and are familiar with to change an attachment from an unacceptably large size, to an acceptable size.
- Save the file in html format and send it.
- Send a shortcut or URL Link to a document or web page rather than the actual document when you are sure the recipients share the same file service on a local server.
- Save a large document as a series of smaller documents and send in stages.
- Avoid sending large images in the attachments, for example a bitmap logo in a Word Document.
- Make sure any necessary picture files are saved as .gif or .jpg, and preferably compressed or sent separately.
- Only use logos, decorative borders and pictures when absolutely necessary.

3. Storage and Archiving - Mailbox Management and Off-line Storage

When a message is sent to an e-mail address it is automatically stored in the associated mailbox.

All Departmental mailboxes have an established size limit which is 7GB and is assigned by Google. Users will need to regularly monitor, store or cull e-mails they have received.

The use of personal and public folders enables you to store important e-mails to reference at a later date whilst still adhering to the mailbox size limit restrictions. As the messages are not stored in your mailbox but on a separate server or area on the e-mail Server, the messages stored do not affect the size of your mailbox. This process of storage is referred to as off-line storage. You have the control of manually selecting and storing e-mail messages that need to be kept.

Public and personal folders allow you to store e-mails that are important to your work. Public folders are a repository for e-mails which are of significance to, and need to be shared with, other employees and individuals within your branch, or the organisation as a whole.

Storing e-mails with attachments fills up a mailbox rapidly. The best way to store messages with attachments is to save the attachment on a networked or local drive, delete the attachment from the message and then store the actual message offline, if required. It is important to ensure that copies of the attachments are not being saved by other employees and individuals. For efficiency purposes, only one copy of a document should be saved.

It is important that you delete any e-mail messages that you no longer need to reference.

To ensure that personal use of e-mail does not result in additional costs to the organisation, non-work related messages (e.g. jokes, messages from family or friends) should not be stored on the e-mail server; messages of this type should be immediately removed after they have been read and dealt with.

4. Responding to Unsolicited and Inappropriate E-mail and Other Material

Inappropriate or offensive e-mail received by employees and individuals, usually falls into one of two categories;

- E-mail that you personally find offensive or that is used to harass you in a directed, specific manner; or
- E-mail that is sent as part of a mass mail out from a person unknown to you (commonly referred to as “spam”).

For further information relating to spam e-mail, please refer to the “Spam” section of this Policy following.

If the e-mail is directed at you as an individual you will need to keep the message and any attachments as evidence and:

- Advise the sender not to send such material to you again; or
- Ask your Campus Manager to advise the sender not to send such material to you again; and
- Report the incident to the Central IT.

5. Leave Procedures

Employees and individuals on extended leave such as annual leave or long service leave, or staff on sick leave of more than two days, must normally make provision for their e-mail to be dealt with during their absence, either through;

- Redirection of their e-mail to another employee or individual, or their manager; or
- Advise of their absence and provide alternate contact details through an out-of-office reply.

6. Generic Addresses

Some business units within the institution have a need for generic e-mail addresses. These are normally general mailboxes that can be monitored by a number of personnel, as opposed to the usual personal e-mail mailbox that each employee or individual receives.

Generally a generic e-mail address is used when a business unit provides a general service that is not specific to a particular person or position within our organisation.

All owners of generic e-mail accounts must ensure that they are checked daily.

7. E-mail Management

SAE Institute tracks and logs e-mail traffic for statistical and technical troubleshooting purposes. Additionally the institution has the right to inspect, monitor, or disclose e-mail activities if it suspects illegal or other activity that might affect the organisation or its employees.

Appendix B: E-mail Etiquette

The purpose of these guidelines is to ensure SAE Institute upholds a professional and untarnished representation in the public eye and amongst the staff body. Emails are one of the mediums used within the institution for communication between other employees and the general public.

It is important to always compose professional emails when addressing staff or partners of the institution.

The institution needs to implement etiquette rules for the following three reasons:

1) Professionalism: by using proper e-mail language our company will convey a professional image.
2) Efficiency: e-mails that get to the point are much more effective than badly worded e-mails.
3) Protection from liability: employee awareness of e-mail risks can protect our company and yourself from costly law suits.

Below is a list what we consider as the most important e-mail etiquette rules that apply within SAE Institute.

Listed below under sub headings are basic guidelines to remember when composing an email. Emails can quite often at times be taken out of context and it is important to make sure these guidelines are prevalent in your emails.

1. Be concise and to the point

Do not make an e-mail longer than it needs to be. Remember that reading an e-mail is harder than reading printed communications and a long e-mail can be very discouraging to read.

2. Answer all questions, and pre-empt further questions

An e-mail reply should answer all questions, and pre-empt further questions. If you do not answer all questions in the original e-mail, you will receive further e-mails regarding the unanswered questions, which will not only waste your time and your client's time but also cause considerable frustration.

Moreover, if you are able to pre-empt relevant questions, your recipient will be grateful and impressed with your efficient and thoughtful client service.

3. Use proper spelling, grammar & punctuation

This is not only important because improper spelling, grammar and punctuation give a bad impression of your company, it is also important for conveying the message properly.

E-mails with no full stops or commas are difficult to read and can sometimes even change the meaning of the text. And, if your program has a spell checking option, why not use it?

Do not use abbreviated words like “wld u pls” or what is becoming more common, the use of abbreviated “SMS message” style communication: e-mail is a full text medium and should be used as such, and may be reproduced in meetings or records of decisions.

4. Make it personal

Not only should the e-mail be personally addressed, it should also include personal i.e. customised content. For this reason auto replies are usually not very effective. However, templates can be used effectively in this way.

5. Use templates for frequently used responses

The most commonly used template in the institution is probably the use of “Out of Office” and should be used in all instances of extended time away from the office. Some people prefer not to use e-mail to schedule meetings; this can be done by using the scheduling function in calendar for all meetings.

This can eliminate excessive responses in trying to find a suitable time, can insure that your calendar is up to date and accurate with your whereabouts, and may reduce effort for other users.

6. Try to respond and reply swiftly

Clients and students send an e-mail because they usually wish to receive a quick response.

Therefore, wherever possible each work-related e-mail should be replied to within at least 48 hours and, whenever possible, preferably within the same working day.

If the e-mail is complicated, just send an e-mail back saying that you have received it and that you will get back to them. This will normally put the client's mind at rest and this can facilitate and encourage further patience.

7. Do not attach unnecessary files

By sending large attachments you can annoy clients, clog up their mailboxes which may have size limitations, and may even bring down their e-mail system. Wherever possible try to compress attachments and only send attachments when they are productive. Moreover, you need to have a good virus scanner in place since your clients will not be very happy if you send them documents full of viruses!

8. Use proper structure & layout

Since reading from a screen is more difficult than reading from paper, the structure and lay out is very important for e-mail messages. Use short paragraphs and blank lines between each paragraph. When making points, number them or mark each point as separate to keep the overview.

9. Do not overuse the high priority option

We all know the story of the boy who cried wolf. If you overuse the high priority option, it will lose its function when you really need it. Moreover, even if a mail has high priority, your message may come across as slightly aggressive if you flag it as 'high priority'.

Your priorities don't always have higher priority than someone else's, and your haste is not always someone else's problem to be welcomed. Give a reason.

10. Do not write in CAPITALS

IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING.

This can be highly annoying, may appear abrasive, and might trigger an unwanted response in the form of a flame mail. Therefore, try not to send any e-mail text in capitals.

11. Don't leave out the message thread

When you reply to an e-mail, you must include the original mail in your reply, in other words click 'Reply', instead of 'New Mail'. Some people say that you must remove the previous message since this has already been sent and is therefore unnecessary. However, opinions vary. If you receive many e-mails you obviously cannot remember each individual e-mail.

This means that a 'threadless e-mail' may not provide enough information and you will have to spend a frustratingly long time to find out the context of the e-mail in order to deal with it. Leaving the thread might take a fraction longer in download time, but it can save the recipient much more time and frustration in looking for the related e-mails in their inbox.

12. E-mail disclaimers

It is important to add disclaimers to your internal and external mails, since this can help protect our organisation and yourself from liability.

13. Read the e-mail before you send it

A lot of people don't bother to read an e-mail before they send it out, as can be seen from the many spelling and grammar mistakes contained in e-mails. Apart from this, reading your e-mail through the eyes of the recipient will help you send a more effective message and avoid misunderstandings and inappropriate comments. It is also usually the last filter for good sense, effective communication and courtesy.

14. Do not overuse Reply to All

Only use Reply to All if you need your message to be seen by each person who received the original message.

15. Take care with abbreviations and emoticons

In business e-mails, try not to use abbreviations such as BTW (by the way) and LOL (laughing out loud). The recipient might not be aware of the meanings of the abbreviations and in business e-mails these are generally not appropriate. The same goes for emoticons,

such as the smiley :-). If you are not sure whether your recipient knows what it means, it is better not to use it.

16. Be careful with formatting

Remember that when you use formatting in your e-mails, the sender might not be able to view formatting, or might see different fonts than you had intended. When using colours, use a colour that is easy to read on the background you have selected.

17. Take care with rich text and HTML messages

Be aware that when you send an e-mail in rich text or HTML format, the sender might only be able to receive plain text e-mails. If this is the case, the recipient will receive your message as a .txt attachment. Most e-mail clients however, are able to receive HTML and rich text messages.

18. Do not forward chain letters

Do not forward chain letters. We can safely say that all of them are hoaxes. Just delete the letters as soon as you receive them.

19. Do not request delivery and read receipts

This will almost always annoy your recipient before he or she has even read your message. Besides, it usually does not work anyway since the recipient could have blocked that function, or his/her software might not support it, so what is the use of using it? If you want to know whether an e-mail was received it is better to ask the recipient to let you know if it was received eg “Please confirm receipt”.

20. Do not ask to recall a message

Biggest chances are that your message has already been delivered and read. It is better just to send an e-mail to say that you have made a mistake. This will look much more honest than trying to recall a message.

21. Do not copy a message or attachment without permission

Do not copy a message or attachment belonging to another user without permission of the originator. If you do not ask permission first, you might be infringing on copyright laws.

22. Do not use e-mail to discuss confidential information

Sending an e-mail is like sending a postcard. If you don't want your e-mail to be displayed on a bulletin board, don't send it. Moreover, never make any libellous, sexist or racially discriminating comments in e-mails, even if they are supposed to be a joke.

23. Use a meaningful subject

Try to use a subject that is meaningful to the recipient as well as yourself.

24. Use active instead of passive

Try to use the active voice of a verb wherever possible. For instance, 'We will process your order today', sounds better than 'Your order will be processed today'. The first sounds more personal, whereas the latter, especially when used frequently, sounds unnecessarily formal.

25. Avoid using URGENT and IMPORTANT, unless really necessary

Even more so than the high-priority option, you must at all times try to avoid these types of words in an e-mail or subject line. Only use this if it is genuinely a very urgent or important message and your recipient will know why.

26. Avoid long sentences

Try to keep your sentences to a maximum of 15-20 words. E-mail is meant to be a quick medium and requires a different kind of writing than letters. Also take care not to send e-mails that are too long. If a person receives an e-mail that looks like a dissertation, chances are that they will not even attempt to read it!

27. Don't send or forward e-mails containing libellous, defamatory, offensive, racist, terrorist, harassing, derogatory, or obscene remarks

By sending or even just forwarding one libellous, or offensive remark in an e-mail, you and our organisation can face court cases resulting in substantial penalties. An e-mail is a publication.

28. Don't forward virus hoaxes and chain letters

If you receive an e-mail message warning you of a new unstoppable virus that will immediately delete everything from your computer, this is most probably a hoax. By forwarding hoaxes you use valuable bandwidth and sometimes virus hoaxes contain viruses themselves, by attaching a so-called file that will stop the dangerous virus.

The same applies for chain letters that promise incredible riches or ask your help for a charitable cause. Even if the content seems to be bona fide, the senders are usually not. Since it is impossible to find out whether a chain letter is real or not, the best place for it is the recycle bin.

29. Keep your language gender neutral

In this day and age, avoid using sexist language such as; 'The user should add a signature by configuring his e-mail program'. Apart from using he/she, you can also use the neutral gender; ''The user should add a signature by configuring the e-mail program'.

30. Don't reply to spam

By replying to spam or by unsubscribing, you are confirming that your e-mail address is 'live'. Confirming this will only generate even more spam. Therefore, just hit the delete button or use e-mail software to remove spam automatically.

In the case of electronic mail, spam is any electronic mail message that is:

- Transmitted to a large number of recipients; and
- Some or all of those recipients have not explicitly and knowingly requested those messages.

It does not really matter what the content of the message is. It can be an advertisement for a commercial product, a solicitation for donations by a charity, or a religious pitch by somebody intent on saving your soul. If it meets the two criteria above, it is probably spam.