F1.1 SGA Use of Technology Policy

Back to Index

See also:
Code of Conduct for E-mail access to SGA accounts of co-workers
Social Media Policy
Public Relations and Media Policy

Policy

It is the policy of Study Group to be clear on the acceptable use of communications technology within our organisation.

Email and Internet access, computers, telephones, voice mail and other technologies are facilities provided for the conduct of Company business.

Scope

The policy applies to all employees and their use of e-mail, Internet, computers, telephones, voice mail and related systems within Study Group.

The policy also applies to contractors, external consultants, vendors or others using e-mail, Internet, computers, telephones, voice mail and related systems within Study Group.

Objectives

To provide guidelines for users of e-mail, Internet, computers, telephones, voice mail and related systems, within Study Group.

Procedure

E-mail

Legal status

E-mail can have the same status as a letter or memo. It is potentially a formal means of communication and should be composed with the same care as a hard copy written document.

Messages which could be construed as obscene, racist, discriminatory, harassing, or that disseminate confidential company information, are expressly banned.

Frivolous communications which unreasonably consume users' time or Study Group's network resources (for example, chain letters, unverified virus reports, lengthy jokes or video/pictorial attachments) are also expressly banned.

Privacy and private use

Users should be aware that, although limited private use is permitted, the system, and all information on it, is the property of Study Group and privacy cannot be assured as all parts of the system can be accessed by some personnel.

In some instances, staff have access to their colleagues e-mail. Please refer to the Code of Conduct for E-mail access to SGA accounts of co-workers.

Study Group is potentially liable for any misuse of the network and has the right to inspect e-mail messages at its discretion. Audits may be carried out on a routine basis to ensure the Company meets its legal responsibilities. (Please refer to Audit and Review below).

If a user is in any doubt as to what is reasonable private use of the system they should ask their manager.

Confidential and proprietary information

Certain types of sensitive or confidential information should not be sent via external e-mail unless adequate security provisions are in place. Any questions concerning whether a particular document or type of document should be sent via e-mail should be directed to the relevant manager.

Social Media

Study Group engages in activities in the social media to grow our profile, direct our brand and extend our leadership. Please refer to *Social Media Policy*.

Employees who are authorised to represent Study Group brands using online social media must follow the guidlines set out in both this Policy and the Public Relations and Media Policy.

Voice Mail

All voice mail messages should be treated as the business communications they are.

As with e-mail messages, Study Group reserves the right to inspect backup copies of messages at any time, within the relevant legal guidelines.

Internet

Use of the Internet for personal interests or business should be kept at a minimum level and should not interfere with business needs.

Viewing or downloading content which could be construed as obscene, racist, discriminatory, harassing or which may lead to dissemination of confidential company information, is expressly banned.

Viewing or downloading frivolous content which consumes users' time or the Company's network resources is also expressly banned.

Study Group is potentially liable for any misuse of the network and has the right to inspect data on computers at its discretion. Audits may be carried out on a routine basis to ensure the Company meets its legal responsibilities. (Please refer to Audit and Review below)

Office Telephones

As with e-mail and the internet, users should be aware that although limited private use is acceptable, the telephone system is the property of the Company and privacy cannot be assured as all parts of the system can be accessed by some personnel.

Study Group is potentially liable for any misuse of the network and has the right to inspect telephone usage at its discretion. Audits may be carried out on a routine basis. (Please refer to Audit and Review below).

If a user is in any doubt as to what is reasonable private use of the system they should ask their manager

All employees should also be aware that wherever practicable, business calls should be made to "land line" telephones rather than mobile telephones. This is partly as a business courtesy to the receiver and also to manage Study Group's operating expenses - calls to mobile telephones are often expensive.

Mobile Telephones

Where the Company does not issue mobile telephones to employees, all employees are requested to submit all business related mobile phone charge claims on the *Expense Claim Form*

The use of personal mobile telephones should be kept to a minimum during working hours.

Where the company does issue a mobile phone to an employee, the use will be confined to business purposes only.

The use of cameras in mobile phones is prohibited within the work environment unless permission is obtained from the employee's manager No external visitors should be allowed to take photographs without permission from a senior manager

Private text messaging should be treated as private telephone calls and emails and be kept at a minimum during working hours.

Use of mobile phones in Company cars must be with a hands-free kit.

Mobile phones must be switched off and not vibrating during meetings and at times where it could be seen as being discourteous or for safety reasons.

Fax Protocol

The rules associated with email traffic also apply to facsimile communications. In addition it is also prudent when sending confidential information by facsimile to advise the recipient prior to sending the document

Unauthorised Software

Study Group is committed to correct software licensing. Installation of any software (unlicensed or otherwise) on the computer network or individual computers which has not been specifically authorised for nominated Study Group employees is expressly banned.

Security & Access

IT allocates each user with an account name and the user sets their own password. Your password is confidential and should not be known to or shared by anyone else.

For security reasons users must not allow their account name and password to be used by anyone other than themselves to gain access to computers and the network or any applications that are provided on the network

Account passwords are required to be changed at least once every **ninety days**. The password chosen must be at least six characters in length and must include at least one number or symbol. Passwords must always be unique and cannot be used more than once.

Guidelines for strong passwords are as follows:

Contain both upper and lower case characters (e.g., a-z, A-Z)
Have number and symbol characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
Are at least six alphanumeric characters long.
Are not a dictionary word.
Are not based on personal information, names of family, etc.
Passwords should never be written down, put on post-it notes on monitors/screens or stored on-line.
Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

Protection for Unattended Computers

To protect confidential information and minimize the risk of unauthorized access, users, when away from their computers for any length of time, should lock their workstation or log off to prevent any unauthorized use.

Misuse of the Systems

Any unlawful or banned use of the systems will result in disciplinary action for employees or possible termination of services of contractors, external consultants, vendors or others.

Employees who become aware of any such misuse, or potential misuse, of the systems should report their concerns to their manager promptly.

Unlawful or banned use of the systems may result in civil or criminal liability for the Company and/or the user.

Audit and Review

The Company has the responsibility to access, audit, review, delete, disclose or use all e-mail, voice mail, telephone accounts and other information stored or transferred on the Company systems, at any time without notice and without recourse regardless of the content of the information, subject to the provisions of applicable local law.

On request from the senior manager/Managing Director, users must provide all passwords or codes necessary to access the user's computers e-mail, voice mail etc.

Use of Study Group' e-mail, voice mail, Internet, computers and related systems constitutes each user's consent to such audit, review and management.

Study Group Category
ANZ-HR-13

Study Group Division

Study Group Department

Study Group Brand

Study Group Region

Study Group Subregion

Study Group Country

Study Group Location

Study Group Faculty

Study Group Important
No

Study Group Status

Study Group Topic

Study Group Note