GEM Compliance Training
First Class First Aid & Safety Training

IT Communication and Monitoring Policy Statement

Introduction

The Employer provides you with access to various IT, telephone and postage facilities ("the Facilities") to allow you to undertake the responsibilities of your position and to improve internal and external communication.

This Policy sets out the Employer's policy on your use of the Facilities. It includes:

- your responsibilities and potential liability when using the Facilities
- the monitoring policies adopted by the Employer, and
- guidance on how to use the Facilities.

This Policy has been created to:

- ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring
- protect the Employer and its employees from the risk of financial loss, loss of reputation or libel, and
- ensure that the Facilities are not used so as to cause harm or damage to any person or organisation.

This Policy applies to your use of:

- local, inter-office, national and international, private or public networks (including the internet and any intranet) and all systems and services accessed through those networks
- desktop, portable and mobile computers, and their applications (including personal digital assistants (PDAs)
- mobile telephones (including the use of WAP and 3G services); and
- electronic mail and messaging services.
-

Observation of this Policy is mandatory and forms part of the Contract of Employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

Computer Facilities - Use of Computer Systems

Subject to anything to the contrary in this Policy the Facilities must be used for business purposes only.

In order to maintain the confidentiality of information held on or transferred via the Employer's Facilities, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Employer's network. Despite your use of a password, the Employer reserves the right to override your password and obtain access to any part of the Facilities.

You are responsible for keeping your password secure. You must not give it to anyone, including colleagues, except as expressly authorised by the Employer.

You are expressly prohibited from using the Facilities for sending, receiving, printing or otherwise disseminating information that is the confidential information of the Employer or its client's other than in the normal and proper course of carrying out your duties for the Employer.

In order to ensure proper use of computers, you must adhere to the following practices:

- anti-virus software must be kept running at all times
- all floppy discs or other forms of media storage must be checked by the nominated IT person before the contents are accessed or stored on the Employer's network or hard drives
- obvious passwords such as birthdays and spouse names etc. must be avoided. The most secure passwords are random combinations of letters and numbers
- when you are sending data or software to an external party by floppy disk always ensure that the disk has been checked for viruses by the nominated IT person before sending it
- all files must be stored on the network drive which is backed up regularly to avoid loss of information, and
- always log off the network before leaving your computer for long periods of time, or overnight.

Software

Software piracy could expose both the Employer and the user to allegations of intellectual property infringement. The Employer is committed to following the terms of all software licences to which the Employer is a contracting party. In particular:

- software must not be installed on any of the Employer's computers unless this has been approved in advance by the nominated IT person. That approval process will establish that the appropriate licence has been obtained, and that the software is virus free and compatible with the computer Facilities
- software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of the nominated IT person.

Laptop Computers

During your employment with the Employer, you may have access to a laptop computer. These computers, along with related equipment and software are subject to all of the Employer's policies and guidelines governing non-portable computers and software (see "Software" section above). However, use of a laptop creates additional problems, especially in respect of potential breaches of confidentiality. When using a laptop:

- you are responsible for all equipment and software until you return it. The laptop must be kept secure at all times
- you are the only person authorised to use the equipment and software issued to you
- you must not load or install files from any sources without the nominated IT person inspecting such files for viruses
- all data kept on the laptop must be backed up regularly in order to protect data against theft, mechanical failure or corruption
- you must password protect confidential data on disks or on the hard drive to protect against theft
- if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of the nominated IT person.

- at any time upon the request of the Employer, you will immediately return any laptop, associated equipment and all software to the Employer, and
- if you damage your company laptop including downloading unsafe documents causing a virus, the cost for fixing or replacing may be deducted from your salary.
- if you are using your own laptop to connect with the Employer's network or to transfer data between the laptop and any of the Employer's computers you must ensure that you have obtained prior consent of the nominated IT person, comply with any instructions and ensure that any data downloaded or uploaded is free from viruses.

E-mail (internal or external use)
Internet e-mail is not a secure medium of communication – it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by e-mail this should be sent using password-protected attachments.

E-mail should be treated as any other documentation. If you would normally retain a document in hard copy you should retain the e-mail.

Do not forward e-mail messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper containing the same information then do not forward the e-mail.

Your e-mail inbox should be checked on a regular basis.

As with many other records, e-mail may be subject to disclosure in litigation. You should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

If you are using e-mail for private purposes then you must ensure that it is not sent on the Employer's template or alternatively ensure that it contains the following message:

- "This e-mail does not reflect the views or opinions of GEM Compliance Training Limited"

Use of e-mail facilities for personal use is permitted during your lunch break, provided that:

- e-mails do not contain information or data that could be considered to be obscene, racist, sexist, otherwise offensive and provided that such use is not part of a pyramid or chain letter, and
- e-mails are not used for the purpose of trading or carrying out any business activity other than Employer's business.

If you are away from the office and use e-mail as an external means of communication you must ensure that the autoreply service is used to inform the sender that you are unavailable. Failure to do so could lead to disciplinary action. Ask for assistance if you have any doubt as to how to use these Facilities.

Viewing, displaying, storing (including holding data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment. It may be illegal. Such use of the Facilities is strictly

prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Internet

Use of the internet, or internet services, by unauthorised users is strictly prohibited. You are responsible for ensuring that you are the only person using your authorised internet account and services.

Downloading any files from the internet using the Facilities is not permitted. If there is a file or document on the Internet that you wish to acquire, contact the nominated IT person to make arrangements for it to be evaluated and checked for viruses. It will be at the discretion of the IT Department on whether to allow such download.

Viewing, downloading, storing (including holding data held in RAM or cache) displaying or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment. It may be illegal. Such use is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Posting information on the internet, whether on a newsgroup, via a chat room or via e-mail, is no different from publishing information in a newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting, and the Employer, could face legal claims for monetary damages.

Using the internet for the purpose of trading or carrying out any business activity, other than Employer's business is strictly prohibited.

Subject to the above, you are allowed to use the internet for personal use during your lunch break. Use of the internet for personal use at any other time is strictly prohibited.

For the avoidance of doubt the matters set out above include use of WAP and 3G facilities.

Monitoring Policy

The Policy of the Employer is that use of the Facilities may be monitored.

The Employer recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities.

The Employer may from time to time monitor the Facilities. The principal reasons for this are to:

- detect any harassment or inappropriate behaviour by employees, ensure compliance with contracts of employment and relevant policies, including the health and safety and equal opportunity policies
- ensure compliance with this Policy
- detect and enforce the integrity of the Facilities, and any sensitive or confidential information belonging to or under the control of the Employer

- ensure compliance by users of the Facilities with all applicable laws (including Data Protection legislation), regulations and guidelines published and in force from time to time; and
- monitor and protect the well-being of employees.

The Employer may adopt at any time a number of methods to monitor use of the Facilities. These may include:

- recording and logging internal, inter-office and external telephone calls made or received by employees using its telephone network (including mobile telephones). Recording may include details of length, date and content
- recording and logging the activities by individual users of the Facilities. This may include opening e-mails and their attachments, and monitoring internet usage, including time spent on the internet and web sites visited
- physical inspection of individual user's computers, software and telephone messaging services
- periodic monitoring of the Facilities through third-party software, including real-time inspections
- physical inspection of an individual's post
- archiving information obtained from the above, including e-mails, telephone call logs and internet downloads.

If at any time an employee wishes to use the Facilities for private purposes without the possibility of such use being monitored he or she should contact their direct supervisor or the person to whom their supervisor reports. This person will consider such request and any conditions upon which such consent is to be given. In the event that such request is granted the Employer (unless required by law) will not monitor the applicable private use.

The Employer will not (unless required by law):

- allow third parties to monitor the Facilities, or
- disclose information obtained by such monitoring of the Facilities to third parties (other than the Employer's legal advisers, and statutory bodies having a legitimate interest in e-mail and internet usage).

The Employer may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

General Guidance

Never leave any equipment or data (including client files, laptops, computer equipment, mobile phones and PDAs) unattended on public transport or in an unattended vehicle.

When using e-mail or sending any form of written correspondence:

- be careful what you write. Never forget that e-mail and written correspondence are not the same as conversation. They are a written record and can be duplicated at will
- use normal capitalisation and punctuation. Typing a message all in capital letters is the equivalent of shouting at the reader
- check your grammar and spelling and

- do not forget that e-mails and other forms of correspondence should maintain the high standards expected by the Employer. Where applicable you should use formal headings and introductions such as “Dear…” and” Yours sincerely” etc.

This Procedure has been approved & authorised by:

Name:	Gavin Milligan
Position:	Managing Director
Date:	01/09/2022
Signature:	

Revisions

Version	Date Created	By	Reason for change
1	1st September 2017	Gavin Milligan	New document
2		Gavin Milligan	