Information Security: User Responsibilities Policy

Please read the policy details and action using the options at the end of the policy.

Table of Contents

1. Definitions

The Company: Refers to Nurture Fostering

The System: Refers to use of e-mail, Intranet and Internet or any of the Company Computer or Telecommunication systems.

ICT: Refers to Information and Communication Technology

The Devices: Refers to any external and portable device capable of being attached to ICT equipment to hold or store data e.g. CDs, DVDs, PDAs, phones, USBs, disks, memory sticks, from time to time.

2. Policy

The Company considers the integrity of its computer system essential to the success of its business. Its policy is to take any measures it considers necessary to ensure that all aspects of the System are fully protected.

The use of the e-mail system and the Internet within the Company is encouraged and its appropriate use facilitates communication as well as improved efficiency. Used correctly, it is a facility that is of assistance to many employees. Its inappropriate use causes many problems from minor distractions to legal claims against the Company. This policy sets out the Company's view on the correct use of the System and explains how this can be achieved, as well as the Company's attitude to inappropriate use.

If you or anyone you allow access to the System (who has no legitimate and agreed rights to access the system) violates this policy your account will be withdrawn and in addition you may be subject to disciplinary action up to and including dismissal.

E-mail messages created and transmitted on Company Devices are the property of the Company. The Company reserves the right to monitor all e-mail transmitted and received via the Company's ICT systems. Employees have no reasonable expectation of privacy when it comes to business and personal use of the Company's e-mail system.

The Company reserves the right to monitor, inspect, copy, review and store at any time and without notice any and all usage of e-mail, and any and all files, information, software and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with employee usage. The Company reserves the right to disclose e-mail text and images to regulators, the courts, law enforcement and other third parties without the employee's consent.

3. Responsibility and Training

3.1. Overall computer security is the responsibility of the IT Manager, reporting to the Director. Managers are responsible for security and management within their own department
3.2. The credentials of all temporary, freelance and consultancy staff should be checked in as much detail as possible before they are allowed access to the ICT system. Managers are responsible for ensuring that all such workers have received a copy of this policy document and understand its contents, and that they have received and signed a copy of the NGH Confidentiality and Non-Disclosure agreement.

3.3. ICT training at every level will emphasise the importance of security.

3.4. Managers are responsible for ensuring that basic procedures are followed. Procedures may be by-passed only with the consent of the Manager and a written record must be kept.

3.5. Training programmes, to familiarise new employees with the System and their uses, will be run regularly on an in-house basis. Managers are required to ensure that all new employees attend the relevant training programme prior to using the System.

3.6 Employees, temporary, freelance and consultancy staff must report any security breaches or suspected security weaknesses in writing to the relevant Manager, Director or to the Security Officer.

4. Security

4.1. Employees of all grades are permitted access only to those parts of the System that they need in order to carry out their normal duties. Levels of access will be decided by Managers in conjunction with the I.T. department, who will ensure that levels of access are consistent and appropriate throughout the organisation.
4.2. In the interests of data security, systems should be locked when unattended and passwords must be used at all times and should be changed regularly. Employees should not select obvious passwords, and where possible they should include both letters and numbers. Passwords must not be disclosed to anyone. Passwords should not be written down, or communicated by telephone, email or instant message. Should you suspect a password may have been compromised, it should be changed. Access to the System using another employee's password without prior authorisation may lead to disciplinary action.

4.3. When an employee is given a temporary password to a higher level of access than he or she normally uses, that password must be cancelled after the individual ceases to need it.

4.4. Employees releasing protected information via a social networking site, web blog or forum, whether or not the release is inadvertent, will be subject to all penalties under existing data security policies and procedures.

4.5. Data held locally (i.e. on your PC's local hard drive) is not backed up as part of the corporate back up process. The user must ensure that a backup is performed satisfactorily, if necessary.

4.6. The IT department ensures e-mails are backed up and stored

4.7 The safe keeping of Devices sent from external sources is the responsibility of the person to whom the Device was sent. All such Devices must be authorised and checked for viruses before use. Devices generated internally must be kept in a safe place.

4.8 It is the responsibility of the IT department to ensure that all back up media is stored off site where applicable.

4.9. Company security will be regularly reviewed striving constantly to keep pace with legislation and technology advances.

4.10. All breaches of ICT security must be referred to the relevant Director, Managing Director or to the Security Officer, where appropriate disciplinary actions may ensue. Where a criminal offence may have been committed, the Board of Directors will decide whether or not to involve the police.

4.11. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the relevant Data Protection legislation.

5. Rules and Regulations

5.1. Any software or data downloaded via the Internet into the Company network becomes the property of the Company. The Company retains the copyright to any material posted to any social networking site, web blog, forum, or World Wide Web page by any employee in the course of his or her duties.
5.2. No employee may use Company facilities knowingly to download or distribute pirated software or data.

5.3. No employee may use the Company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, key logger, or trap-door program code.

5.4. Access to the Internet is strictly limited: no personal surfing is permitted. Access to the Internet for business purposes is permitted. Limited access for personal use is also permitted provided that it is done outside normal working hours and ensuring that all other usage policies are adhered to.

5.5. No employee may use the Company's Internet facilities to deliberately download, distribute or propagate material of an inappropriate nature. e.g. pornography, jokes etc.

5.6. No private work or computer game playing is permitted.

5.7. Only those employees or officials who are duly authorised to communicate to the media, to analysts or in public gatherings (chat sites etc.) on behalf of the Company, may speak/write in the name of the Company, to any newsgroup, chat room or similar.

5.8. Employees with Internet access may download only software with direct business use, and must arrange to have such software properly licensed and registered and virus checked. Downloaded software must be used only under the terms of its license.

5.9. Employees with Internet access may not use Company Internet facilities to download entertainment software or games, or to play games either singly or against opponents over the Internet, or access/use gambling sites.

5.10. Employees with Internet access may not upload any software licensed to the Company or data owned or licensed by the Company without explicit written authorisation from the Manager responsible for the software or data.

5.11 All software must formally be authorised before being installed on Company systems by the Network Manager/IT Director. No external software or data originating outside the Company may be used without authorisation by both a Manager of the IT Department and/or the employee's Manager.

5.12 Non company Devices (i.e. users' own Devices) may not be connected into the Company network in any way whatsoever without prior written authorisation from the Network Manager/IT Director.

6. Mis-use of the System

6.1. Mis-use of the System is a serious disciplinary offence. The following are examples of mis-use: -

a) fraud and theft;

b) deleting business e-mails, inappropriately, before being archived;

c) system sabotage;

d) introduction of viruses, key loggers and time bombs;

e) using unauthorised software;

f) obtaining unauthorised access;

g) using the System for private work or playing games;

h) breaches of the Data Protection legislation;

i) sending abusive, rude or defamatory messages by electronic mail;

j) hacking;

k) breach of Company security procedures.

This list is not exhaustive. Mis-use of the ICT System is likely to be considered a gross misconduct offence, punishable by dismissal, depending on the circumstances or severity of each case. Use of any Company resources for illegal activity is grounds for immediate dismissal, and the Company will co-operate with any legitimate law enforcement activity.

6.2. The Company has policing software which may change from time to time to enable monitoring and management of use/misuse of the IT systems.

6.3. Any member of staff who suspects that a fellow employee, of whatever seniority, is abusing the ICT System, may speak in confidence to the HR Function.

7. E-Mail and Internet Guidelines

The e-mail system and the Internet are available for communication directly concerned with the business of the Company. Employees using e-mail or Internet systems should give particular attention to the following points:

7.1. **The Standard of Presentation**

The style and content of an e-mail message must be consistent with the standards the Company expects from written communications.

7.2. **The Extent of Circulation**

E-mail messages should only be sent to those employees/clients/applicants/suppliers for whom they are relevant. E-mailing all group employees with inappropriate communications is considered a serious mis-use of the System, as is failure to consider the impact of the communication, which in itself may be inappropriate, on network usage and its affect on other users (eg bandwidth wastage).

7.3. **The Appropriateness of E-mail**

E-mail should not be used as a substitute for face to face communication. Abuse of e-mails can be a source of stress and can damage work relationships. Hasty messages, sent without proper consideration, can cause unnecessary mis-understandings.

7.4. **Visibility of E-mail**

If the message is confidential, the user must ensure that the necessary steps are taken to protect confidentiality. The Company may be liable for any defamatory information circulated either within the Company or to external users of the System.

7.5**. E-mail Contracts**

Offers or contracts transmitted by e-mail are legally binding on the Company as though sent on paper, and appropriate copies must be retained and filed.

7.6**. Prohibited Use**

The Company will not tolerate the use of the System for any of the following:-

a) any message that constitutes bullying or harassment (e.g. on the grounds of sex, race or disability);

b) The personal use and/or creation of any social networking site, web blog or forum (such as facebook, myspace, bebo) is strictly prohibited during working hours. If these forums are used during the working day, albeit during personal time (e.g. lunchtime), it is also strictly prohibited to share, comment or act in representation of the Company, its business affairs, employees, customers or any other associated parties. This extends without exception to any details and resources used that could associate you to the aforementioned parties (e.g. use of Company email address).

Should the Company ever need to set up a Web Blog or Forum, it must be made formally by request through the requestor's line management channels, at which point rules and regulations of usage will be set.

c) on-line gambling;

d) viewing, downloading or distributing pornography or other offensive material;

e) downloading or distributing copyright information and/or any software available to the user;

f) posting confidential information about other employees, the Company or its customers or suppliers.

8. General

8.1. The IT Director will be responsible for the management of the System. This person will be available for advice on all technical aspects of the policy. The HR Function will manage all other aspects.

8.2. The Network Manager will carry out regular monitoring of e-mail messages on a random basis. Hard copies of e-mail messages will be used as evidence in disciplinary proceedings.

8.3. The Company reserves the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

8.4. Employees who feel that they have cause for complaint as a result of e-mail communication should raise the matter initially with their Manager. If necessary, the complaint can then be raised through the grievance procedure.

These guidelines are intended to provide Company employees with general examples of acceptable and unacceptable use of the Company’s systems. A violation of this policy may result in disciplinary action up to and including termination.