LOGO

Acceptable Computer Use and Electronic Communication Policy for Company Name

1. Purpose

To ensure that employees understand the guidelines governing computer use: Internet access, email, other electronic communications, software licensing, security and personal use, in particular.

This policy cannot lay down rules to cover every possible situation. Instead, it is designed to express COMPANY NAME's (COMPANY ABBREVIATION) philosophy and set out the general principles that employees should apply when using company computers and technology. These policies apply to all COMPANY NAME employees & staff (Doctors, PAs, Technicians, Providers, Third-Party Contractors, and Administrators).

This policy does not cover health and safety issues.

Issues not directly addressed in this policy or in some other written form are to be decided by HR and/or IT Departments should the need(s) and situation(s) arise.

HIPAA and its related acts and laws are the final authority governing these policies. If any portion of this policy is in conflict with or not specified herein, HIPAA procedures take precedence unless COMPANY NAME policy take a stricter position. In summary, the stricter guideline/rule/policy wins any policy conflict.

As a general reminder, the HITECH act makes HIPAA violations/violators personally liable. Should a violation of HIPAA occur you may be personally held liable in any civil or criminal form.

Unless otherwise stated, violation of these polices will result in disciplinary action, including and possibly up to termination and/or legal action. (See Section 17 for complete details)

2. General

COMPANY NAME provides employees and staff with PCs, printers and other computer equipment as necessary to perform their job. In general, equipment is selected on the basis of its suitability for purpose, not by its age or version number. Employees should not expect the latest hardware or software releases to be provided unless there is a business reason to do so.

COMPANY NAME encourages the use of email, voicemail, online services, the Internet and intranet because they can make communication more efficient and effective. In addition, they can provide valuable sources of information about vendors, customers, technology, and new products and services.

Everyone connected with the organization, however, should remember that electronic media and services provided by the company are company property and their purpose is to facilitate and support company business.

Data stored or accessed on company equipment, regardless of origin, purpose or design should also be considered to be within, at least, company purview, oversight and audit rights. The company reserves the right to access data, of any sort, stored or located on company provided equipment.

3. Email/Communications

All employees and staff are supplied with a company email address and the means to which access their account. These details are provided by the IT department.

All non-company email services, such as Gmail, Hotmail, Yahoo!, etc. are never to be used for company purposes, pursuant to HIPAA regulations and requirements. If third-party email services must be utilized, it will be provisionally and under direct supervision of the IT department. Never is an employee or staff member to use a personal email account to correspond with patients.

Electronic media (email, web browsers, etc.) must not be used for knowingly transmitting, retrieving, or storing any communication that:

- Is discriminatory
- Is harassing or threatening
- Is derogatory to any individual or group
- Is obscene or pornographic
- Is defamatory
- Is engaged in any purpose that is illegal or contrary to COMPANY NAME's policy or business interests.
- Contains unencrypted Protect Health Information (PHI)

Further, all forms of mass email (including 'virus warnings', 'good luck' and similar messages) are unacceptable, unless for an approved business purpose.

The transmission of user names, passwords or other information related to the security of COMPANY NAME's computers is not permitted.

Employees should avoid sending unnecessary informational emails to large parts or all of the organization. Common area bulletin boards should be used for all solicitation messages (items for sale, for example). However, we do recognize the business need for wide emails, but there will be a strictly monitored and governed use of such a behavior and practice.

Furthermore, direct communication with patients via email is strongly discouraged unless proper HIPAA procedures are followed and practiced, such as: encrypting email messages that contain Protected Health Information (PHI) and/or personally identifiable information, properly logging the interaction in the company EMR, and reporting all medical emergencies and/or situations through the proper channels.

Under no circumstances should email ever be used to diagnose or treat patients.

All email is archived in a searchable database, pursuant to HIPAA requirements, and will be retained for a minimum of five years or as regulations dictate.

4. External email and participation in online forums

Employees should be aware that any messages or information sent using the company systems are statements identifiable and attributable to the company. Thus, an email carries the same weight in law as a letter written on headed company paper.

Employees should note that even with a disclaimer, which is utilized in official company electronic communication, a connection with the company still exists and a statement could be imputed legally to COMPANY NAME. Therefore, no one should rely on disclaimers as a way of insulating COMPANY NAME from the comments and opinions that are contributed to forums or communicated in emails. Instead, discussions must be limited to matters of fact and expressions of opinion should be avoided while using company systems or a company-provided account. Communications must not reveal information about company processes, techniques, trade secrets, or confidential information and must not otherwise violate this or other company policies.

Employees should not send file attachments by email in situations where there is any potential for the compromise of company secrets, Protected Health Information (PHI), or in relation to litigation. Be aware, files from many word-processing packages, including Microsoft Word, retain information relating to previous versions of the document that can be later retrieved.

5. Electronic calendars and voicemail

It is COMPANY NAME policy that all employees keep their electronic calendars up to date (using Microsoft Outlook, Outlook Web Access or approved software) and that calendars can be read by supervisors. Where a meeting or event needs to be kept confidential it should be marked as 'private' with the appropriate program functionality.

It is COMPANY NAME policy that all employees with voicemail keep their pre-recorded greetings up-todate. In particular, during periods of absence from the office, the voicemail greeting should provide the caller with information indicating when the employee will receive a message and information about an alternative contact.

6. Software licenses

It is policy that only licensed software that is legally owned by the company may be used. All use of unlicensed software is expressly forbidden.

In order to implement this policy, COMPANY NAME maintains a central register containing all the physical licenses for the software installed on its computers. Where no physical manifestation of a license exists, a written record of the license purchased is kept with a reference to the relevant invoice. It is the responsibility of the IT support organization to maintain this license repository.

Free or shareware programs should not normally be installed on company computers due to the risk of virus infection and other side effects. Where installed, they are only exempt from the central license recording provided that the software clearly identifies itself as free.

7. Standard configuration

Standard hardware and software configurations are used wherever possible to provide the best possible levels of reliability for the company network and computers. Other benefits of the standard configurations include the rapid replacement of faulty equipment with spare parts, the tracking of software licenses (as described in the preceding section) and the ability to plan for the implementation of new projects.

v1.2

The configuration of company computers should not be changed in any way without the prior agreement of the IT department. In particular, new hardware devices, new software and upgrades to existing software should only be installed under the guidance of the IT department.

8. Physical security

Employees issued portable (laptop, tablet) computers must take reasonable precautions. When out of the office, the computer should always be under direct control of the employee or out of sight in a secure location. COMPANY NAME may also take other security measures including, but not limited to, computer tracking hardware/software, security cables, and/or hard drive encryption.

9. Data security

All employees/contractors are assigned a network user name and password when joining the company. The network will force employees/contractors to change their password at regular intervals, the interval being determined by the network administrator. The network administrator will also impose other restrictions, such as a minimum password length and complexity requirements. The current required minimums are 6-64 characters (a-z) including one number (0-9) and one special character (capital letters, !, @, #, \$, etc.), e.g. Appl3tr33.

Employees must select network passwords that cannot be easily guessed. If it is necessary to create a written record of a password, then that record should never be stored near the employee's desk and never associated with the employee's user name. In general, passwords should be memorized and not recorded in writing.

10. Privacy

COMPANY NAME respects your desire to work without the company being overbearing in respects to monitoring and control. However, detailed electronic records about your use of the PC, the network, email, and Internet are created, but not routinely reviewed by the company.

While company does routinely gather logs for most electronic activities, they will typically be used for the following purposes:

- cost analysis
- resource allocation
- optimum technical management of information resources
- detecting patterns of use that indicate users may be violating company policies or engaging in illegal activity.

COMPANY NAME reserves the right, at its discretion, to review any electronic files, logs and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other company policies. This includes the use of spot checks on Internet (Web) use, network files and email without prior notification or user interaction.

Software tools to identify possible breaches of this policy (e.g. highlighting access to websites with unacceptable content or emails containing abusive language) may be used. The results will be reported to the company management and thoroughly investigated where appropriate.

It should not be assumed that internal or external electronic communications are totally private. Accordingly, particularly sensitive information should be transmitted by other means. Therefore, do not use the company network for personal items that you would not want to be made public.

11. Encryption

Only encryption software supplied by the IT department for purposes of safeguarding sensitive or confidential business information may be used. People who use encryption on files stored on a company computer must provide their manager with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

Power-on passwords should not generally be used but if they are, a copy must be given to the IT department.

Please note: this means that employees must inform their supervisor of any passwords used to protect individual documents.

12. File storage

The IT department creates backup images of all email, server and network file stores every night. These images are stored in a secure location and can be used in the event of:

- accidental deletion of important material
- a 'disaster' necessitating complete recovery of one or more of the company's systems.

Data and other files created during the course of an employee's work should, therefore, be stored on the network. However, the company utilizes technology that redirects typical Windows folders (e.g. My Documents, My Pictures, etc.) to a network location, transparently to the users. Therefore, very little action is needed to be done by the user unless directed by the IT department.

13. Personal use

Computers and associated equipment are provided by COMPANY NAME for employees' and staff's business use. Limited, occasional, or incidental use for personal, non-business purposes is understandable.

However, use of company provided computers for access of email by employees for personal, nonbusiness purposes is not acceptable, unless provisionally granted on a per-case basis by HR and/or IT for limited, occasional or incidental use. (i.e. as a guide, 'limited, occasional or incidental use' is taken to mean less than fifteen minutes). Exceptions to this policy are computers provided to staff that are regularly taken home; however, data stored on this equipment is subject to audit and access.

Use of social networking sites (eg. Facebook, MySpace) at any time using company provided computers is strictly forbidden, unless it is for company purposes and/or business. Exceptions to this policy are computers provided to staff that are regularly taken home; however, data stored on this equipment is subject to audit and access.

Personal laptops, cell phones, and other internet enabled items are permitted to be used; however, reasonable restrictions of use may be exercised at HR/IT discretion. COMPANY NAME does not provide internet access for public/private use, except on an approved device/user basis.

v1.2

BUILDING MANAGEMENT, and possibly other locations, typically does/do provide a freely accessible public WiFi connection that may be utilized by employees and staff, but COMPANY NAME absolves itself of any and all damage, liability, etc. that arises from the use of third-party networks. It is the policy of COMPANY NAME that if an employee chooses to utilize these third-party connections that they do so on their break, lunch, or after-hours and do not pursue personal activities during business hours.

14. Contract and freelance staff

COMPANY NAME will provide agency/temporary/contract /freelance staff with access to computers and the company computer systems for the sole purpose of fulfilling their contractual role with COMPANY NAME. No personal use by these staff of computer and communication facilities provided by COMPANY NAME is permitted at any time, without exception.

15. Games

The limited use of games is permitted, though discouraged. The following restrictions apply:

- Games may not be played between 8am and 5pm on normal workdays (or the department's working hours, whichever is the more restrictive).
- Employees may not install games (i.e. only those that are pre-installed are permissible).

16. Viruses/Spyware

All computer viruses/spyware must be reported immediately to the IT support group. The IT support group is responsible for updating virus/spyware detection software from time to time and providing detailed guidelines in the event of a major problem. The IT support group will also investigate any infection and must receive the full co-operation of all staff in attempting to identify the source. Any attempt to introduce viruses/spyware to the network through malice or negligence will be thoroughly investigated and will be dealt with according to HR guidelines and procedures.

17. Policy violations

Employees who abuse the Computer Use and Electronic Communications policy are subject to disciplinary action, up to and including termination of employment, and risk having privileges removed for themselves and other employees. HIPPA violations are punishable by law and those found violating HIPAA and its related acts are subject to personal liabilities in both civil and/or criminal court. COMPANY NAME offers no personal legal shelter for HIPAA violations.

This policy was created: 4/28/2010 This policy was last edited: 5/03/2010 Policy version: 1.2

Current IT Department Administrator: Current HR Department Administrator: