CCEMS
OPERATIONS POLICY 100-19
USE OF COMPUTER AND INFORMATION SYSTEMS AND EQUIPMENT

I. PURPOSE

1.1 CCEMS is committed to protecting our staff members, the patients we serve, and the company from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or propriety information.

1.2 The purpose of this policy is to outline the acceptable use of computer equipment at CCEMS. These rules are in place to protect the employee and patients of CCEMS. Inappropriate use exposes CCEMS to risks including virus attacks, compromise of network systems and services, breach of patient confidentiality, and other legal claims.

1.3 This policy applies to employees, volunteers, contractors, consultants, temporary employees, students, and others at CCEMS who have access to computer equipment, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by CCEMS.

1.4 In addition to this SOP; the Coshocton County Employee Manual Section 8.6 "Computer Policy" also outlines computer policy and will be followed in conjunction with this SOP.

II. POLICY

2.1 All equipment, hardware, software, intellectual property created while employed by or on CCEMS equipment is the property of and belongs to Coshocton County. All equipment and access to software shall be controlled at all times by passwords. All contents of computers shall be regarded as confidential and shall be treated and guarded as such. There are appropriate and inappropriate uses of computers and software, inappropriate uses are strictly prohibited and will result in progressive disciplinary action. The use of computers and software is a privilege that must be maintained and can and will be revoked upon misuse.

III. PROCEDURE

3.1 All data created or recorded using any computer equipment owned, controlled, or used for the benefit of CCEMS is at all times the property of Coshocton County. Because of the need to protect the CCEMS computer network, the company cannot guarantee the confidentiality of information stored on any network device belonging to Coshocton County, except that it will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

3.2 Staff members are responsible for exercising good judgment regarding the reasonableness of personal use and must follow operational guidelines for personal use of Internet/Intranet/Extranet systems and any computer equipment.

3.3 At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any company computer equipment.

3.4 For security and network maintenance purposes, authorized individuals within CCEMS may monitor equipment, systems, and network traffic at any time to ensure compliance with all CCEMS policies.

3.5 Confidential information should be protected at all times, regardless of the medium by which it is stored. Examples of confidential information include, but are not limited to: individually identifiable health information concerning patients, company financial and business information, patient list and reports, and research data. Staff members should take all necessary steps to prevent unauthorized access to this information.

3.6 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed upon direction of the Coshocton County IT Department.

3.7 All PC's, laptops, workstations, and remote devices will be secured with a password, wherever possible, and set to deactivate after being left unattended for ten (10) minutes or more, or by logging-off when the equipment will be unattended for an extended period.

3.8 All computer equipment used by staff, whether owned by the individual staff member or CCEMS, shall regularly run approved virus-scanning software with a current virus database in accordance with company policy.

3.9 Staff members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

3.10 Under no circumstances is a staff member of CCEMS authorized to engage in any activity that is illegal under local, state, or federal law while utilizing CCEMS computer resources.

3.11 The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

3.12 The following activities are strictly prohibited, with no exceptions:

3.12.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or ANY other software products that are not appropriately licensed for use by CCEMS.

3.12.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CCEMS or the end user does not have an active license is strictly prohibited.

3.12.3 Installation of any software without express permission by the county IT Department.

3.12.4 On-line chatting and/or blogging.

3.12.5 Any My-Space account or URL.

3.12.6 Play any on-line games, i.e.; Pogo, Blackjack, on-line casino, etc. The only games permitted are the ones that came installed with Windows XP (Solitaire, Mine Sweep, etc.)

3.12.7 Exporting system or other computer software is strictly prohibited.

3.12.8 Introduction of malicious programs into the network or server, i.e. viruses, worms, etc.

3.12.9 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

3.12.10 Using a CCEMS computer device to actively engage in procuring or transmitting material that is in violation of CCEMS's prohibition on sexual and other harassment.

3.12.11 Making fraudulent statements or transmitting fraudulent information when dealing with patient or billing information and documentation, account or other patient information, including the facsimile or electronic transmission or patient care reports and billing reports and claims.

3.12.12 Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the staff member is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

3.12.13 Providing information about, or lists of, CCEMS staff members or patients to parties outside CCEMS.

3.12.14 Sending e-mail messages, such as "junk mail", non-charitable or other advertising material to individuals who did not specifically request such material (e-mail spam).

3.12.15 Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.

3.12.16 Unauthorized use, or forging, of e-mail header information.

3.12.17 Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

3.12.18 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

3.13 The appropriate use of laptop computers, personal digital assistants, and remote data entry devices is of utmost concern to CCEMS. These devices, collectively referred to as "remote devices" pose a unique and significant patient privacy risk because they may contain confidential patient, staff member or company information and these devices can be easily misplaced, lost, stolen, or accessed by unauthorized individuals.

3.13.1 Remote devices will not be used with or connected to CCEMS's networks or CCEMS equipment without prior Coshocton County IT department approval.

3.13.2 Coshocton County IT must approve the installation and use of any software used with or on the remote device.

3.13.3 Remote devices containing confidential or patient information must not be left unattended.

3.13.4 If confidential or patient information is stored on a remote device, access controls must be employed to protect improper access. This includes, where possible, the use of passwords and other security mechanisms.

3.13.5 Remote devices should be configured to automatically power off following a maximum of ten (10) minutes of inactivity.

3.13.6 Remote device users will not permit anyone else, including but not limited to, user's family and/or associates, patients, patient families, or unauthorized staff members, to use company-owned remote devices for any purpose.

3.13.7 Users of company-owned remote devices will immediately report the loss of a remote device to leadership.

3.14 Computers are for business use only and can only be used for:

3.14.1 Utilizing Microsoft Office programs to complete items related to CCEMS.

3.14.2 Checking weather or 'breaking news.'

3.14.3 Searching the internet for items related to CCEMS

3.15 Checking CCEMS email through the Intranet

3.16 Any staff members found to have violated this policy may be subject to progressive disciplinary action, up to and including suspension and termination.

Director: 

Effective: 09-16-2008

Reviewed: _____

Revised: _____