Acceptable Use Policy

NHS P05

Approval:

Policy Approved by	Date Policy Approved on

Document Change History

Version Number	Release Date	Changes implemented	Sections	Changes implemented by

Table of Contents

Policy Purpose

This policy provides direction to employees, contractors and other users for acceptable use of the Department's computing resources. As a part of the overall information security policies, this policy highlights for employees areas of common acceptable use of the computer resources and expectations of employees for proper use and care of the computer systems.

Policy Statement

1. Internet and Email Policy

- Employees are expected to use the Internet and email responsibly and productively. Internet access is limited to job-related activities and authorized Department business only. Limited personal use is allowed so long as it does not interfere with work duties or disrupt the systems performance and integrity, and abides by the policies set forth herein. (*Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role*).
- All Internet and email data that is composed, transmitted and/or received by Department computer systems is considered to belong to the Department and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services and technology used to access the Internet and email are the property of company and the company reserves the right monitor and access data that is composed, sent or received through its online connections.
- **No expectation of Privacy**: An employee's rights while using the Internet or email via company resources does not include the right to privacy. The company reserves the express right to monitor and inspect the activities of the employee while accessing the Internet or email at any time. In addition, all software, files, information, communications, and messages downloaded or sent via the Internet or email using company resources are the company's records and property of the company.
- All sites, email and downloads may be monitored, filtered and/or blocked by the Department if they are deemed to be harmful and/or not productive to business.
- The installation of non-authorized and non-Department owned software (as determined by the Department, such as instant messaging technology) is strictly prohibited.
- All files downloaded from the Internet must be scanned with anti-virus software approved by the Department.
- No computer used for Internet access can be running peer-to-peer network services.
- No computer used for Internet access can be connected to another Internet Service Provider other than what is provided by the Department.

- Emails sent via the Department email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

2. Mail (Physical Paper) Security

- Mail that likely contains confidential information should be opened by addressee or authorized personnel.
- To the extent mail is received in an envelope that is not addressed to a specific person, where it is unclear that it is from the subject of and may contain confidential information, the mail may be opened by unauthorized staff, provided that person opening the envelope reviews the least amount of contents needed to determine to whom the mail is addressed and/or that it contains, at which time the mail shall be delivered to the appropriate person.
- The following controls shall be established when Confidential information is mailed externally:
  - ➢ The mailing address of the addressee shall be double-checked before sending the mail.
  - ➢ Confidential information must not be visible through the envelope, including any window in the envelope.
  - ➢ Sealed envelope or an envelope that may be securely closed must be used and it shall not be provided to unauthorized staff or third persons until properly sealed or closed.

3. Employee Responsibilities

As users of NHS technology resources, employees have a shared responsibility with the IT Department staff to maintain the integrity of systems, services, and information so that high quality services can be provided to all employees.

Employee responsibilities include:

- Using the Department's technology resources responsibly and appropriately, consistently with the mission and purpose of the Department, and respecting the rights of other users.
- Respecting privacy and maintaining confidentiality of information.
- Understanding the nature of Confidential, Internal Use and Public Information.
- Complying with federal, state, and local regulations regarding access and use of information resources. (e.g. The Family Education Rights and Privacy Act, NIST policies, codes of professional responsibility, etc.).
- Maintaining system accounts (to include files, data and processes associated with those accounts) and PC files, data, and processes, which includes taking appropriate action to backup your PC system.
- Employees should not store confidential data on their local PC system and should store them in shared drives.
- Exercise due diligence in protecting computer you connect to the Department network.

- It is the responsibility of employees to practice "safe computing" by establishing appropriate access restrictions for their accounts, by guarding their passwords, and by changing them regularly. Keep your technology accounts (computer, network) secure.
- To not share privileges with others. Access to technology resources is not transferable to other employees, to family members, or to an outside individual or organization.
- If you suspect unauthorized access, report it to your supervisor or the Information Systems Manager.

4. Installed Software

- All software packages that reside on computers and networks within organization must comply with applicable licensing agreements and restrictions and must comply with organization acquisition of software policies.
- The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the computer systems immediately.
- Employees are prohibited from installing any software, executable, or other file to any Department computing device if that software, executable, or other file was purchased or downloaded for their personal use. Purchased or downloaded software, executable, or other files include, but are not limited to: SKYPE, music files or software, peer-to-peer software and personal photos.

5. Ownership of Software

All computer software purchased and developed by Department employees or contract personnel on behalf of organization or licensed for Department use is the property of the organization and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

6. Data Transfer/Printing

- Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.
- Copy/Printing machine equipped with a memory, that allows the reprinting of a document previously copied, upon completion of the copy/print job involving documents containing confidential information shall be deleted prior to leaving the machine.
- In the event a copy/print containing confidential information is unusable (because it is not dark enough, etc.) it shall be destroyed by shredding.

7. Facsimile Machines security

- Trusted staff members must be identified at both the sending and receiving end when transferring confidential data. Fax machines shall be placed in secure areas.

- Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes: notification of the sensitivity of the data and the need for protection, notice to unintended recipients to report the disclosure and confirm destruction of the information.

8. Confidential Records Security

The following controls shall be implemented to secure physical records that contain confidential information within Program Offices and Region sites:

- Paper records that include confidential information must be secured. All incidents that may involve the loss or theft of any such paper records must be reported to Program Director and Information Systems Manager. Confidential records must be located and used so as to minimize incidental disclosure.
- If the confidential record is in use, but not actively being viewed, it shall be closed, covered or placed in a position to minimize incidental disclosure. This is especially important in Agency sites.
- When confidential records are in transit information shall be covered, so that no personal identifiers are visible to minimize exposure.
- When in storage confidential records must be stored where there is controlled access. Information shall not be stored in open and in hallways where information is accessible by unauthorized individuals. Confidential records shall not be stored in open shelves.
- Confidential records shall be stored out of sight of unauthorized individuals, and shall be locked in a cabinet, room or building when not supervised or in use.
- Provide physical access control for Program offices and Region sites through the following: Locked file cabinets, desks, closets or offices, Keys, electronic ID swipes, keypad systems where codes are changed on a regular basis.
- Management of physical access must be assigned to designated employees within the Program Offices and Region sites. Access must be removed immediately when the employee's role changes or if terminated.

9. Social Networking Policy

- Employees need to understand that with the ability to use social networking comes responsibility.
- Before any information generated by or for the Department is made public it must be reviewed by the Public Information Officer and the Management appointed designee to ensure that it does not contain confidential information.
- Clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the Department shall be explicitly mentioned. Employees

shall be clear and shall write in first person. The writing shall be clear that the employee is speaking for themselves and not on behalf of the Department.

- Information published on social networking sites shall comply with the Department's confidentiality and disclosure of proprietary data policies.
- Social media activities shall not interfere with work commitments.
- The malicious use of online social networks, including derogatory language about any member of the department; demeaning statements about or threats to any third party; incriminating photos or statements depicting hazing, sexual harassment, vandalism, stalking, underage drinking, illegal drug use, or any other inappropriate behavior, will be subject to disciplinary action.
- The Department reserves the right to monitor employee use of social media, monitor, implement controls and block inappropriate web access.
- Sanctions for failure to agree and adhere to this policy will result in actions ranging from reprimand or suspension to dismissal from the Department authorized by the Superintendent or his designee.

10. Verbal Communications

Employees should be aware of their surroundings when discussing confidential information. This includes the use of cellular telephones in public areas. Staff should not discuss confidential information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

11. Unacceptable Use

Unacceptable use of the internal computing resources by employees or other users includes, but is not limited to:

- Access to sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material
- Accessing social networking sites including: blog sites, wiki, Twitter, MySpace, Facebook, LinkedIn, Digg or any other form of online publishing site unless otherwise authorized by management.
- Access to all video and audio streaming sites including, but not limited to: Youtube, HBO and other sites hosting video and content that are counterproductive to business operations.
- Downloading, installing and changing desktop backgrounds and screensavers.
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via company's email service.
- Using company computers to perpetrate any form of fraud, and/or software, film or music piracy.
- Stealing, using, or disclosing someone else's password without authorization.

- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.
- Circumventing or overriding any security mechanism belonging to the company though IT resources and access provided.
- Sending or posting information that is defamatory to the Department, its products/services, colleagues and/or customers.
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organization.
- Altering, stealing customer credit card information.

If an employee is unsure about what constituted acceptable internal resource usage, then he/she should ask his/her supervisor and/or the IT manager for further guidance and clarification.

Policy Acknowledgement

No company employee shall be authorized to use the Department’s internal resources until he or she has signed a document indicating that the employee has read and agrees to be bound by the terms of the information security policies. Upon hiring, each new employee will receive a copy of the Information Security policies. Employees should review and acknowledge these policies within 30 days of hire.

Breach of this policy

Any willful and/or deliberate breach of this policy or other information security policies will be viewed as a serious disciplinary offence and may result in actions up to and including termination of employment for employees. Legal actions also may be taken for violations of applicable regulations and laws under which an offender may be prosecuted or be subject to a claim for damage or distress by a data subject.

Further advice and information

For advice on appropriate security measures or other aspects of this policy, contact the Information Systems Manager.

Acknowledgement

I have read, understood and shall abide by the policies defined in this document. As the Company provides updated policy or procedure information, I accept responsibility for reading and abiding by the changes.

Name (first name last name) ___________________________________

Program Name: ___________________________________

Signature: ________________________________ Date: _______________

This Signature Page is to be completed by the employee and given to the Personnel Department who is responsible for keeping it as a part of the employees personnel file.