INTERNET POLICY

Proper use of the Internet can enhance the learning capabilities of the student. Due to the fact that the Internet is largely unregulated and uncensored, organizations are responsible for establishing appropriate Internet usage guidelines for Internet access.

Responsibility: Students, Program Officials
Standard: Information Management

Introduction: As technology advances, the Internet has become a powerful information resource. Proper use of the Internet can enhance the learning capabilities of the student. This policy explains the acceptable and unacceptable uses of the Internet provided by Regional West Health Services. Use of the Internet for electronic mail (e-mail) is addressed in Electronic Mail (e-mail) Policy #722.8.01.30, Internet security is addressed in Information Security, Policy #722.8.01.05.

Use of the internet will be limited to official department business or academic endeavors. Students are encouraged to use the resources on the Internet to enhance learning opportunities.

Access to Hospital Networks

The students have access to two Internet networks while on campus:

1. Students can gain access to the RWMC network after completing hospital orientation and obtaining a user name and password from the IT department.

2. The guest network from which the student can gain access to the. Wireless Internet access of the "guest" wireless network is permitted for students using personal devices during class or clinical time when used only for educational purposes.

The use of the Sponsoring Institution's Internet systems for personal use is permitted during breaks and outside of class or clinical time.

Report Unauthorized Use

Observation of unauthorized or inappropriate use of the Internet must be reported immediately to a supervisor or Regional West Health Services Security Officer. Detection of external efforts to compromise the system must also be reported to the Security Officer or the Vice President of Information Technology/Chief Information Officer.

Submission of Data

Students must remember that data sent and received over the Internet should be considered "public" and readable by anyone. Special consideration should be taken before transmitting sensitive information, including E-mail and web browser forms.

Encryption techniques must be used to reduce the risk of public access. Consult with Information Systems if there is a question as to the sensitivity of the material.

Copyrighted Data and Files

Data and files on the Internet must be considered copyrighted material and may not be distributed, copied or published in any form without the written permission of the originator (except as detailed in Title 17 of the United States Code, section 107, "Fair Use Doctrine"). Material does not need to have a copyright on it to be protected under U.S. Copyright Law.

Downloading Files From the Internet

Files, of any type, when downloaded from the Internet have the potential of harming the network. Downloading of any file may be blocked by the system's protection tools.

The most dangerous files are those that are actual executable files. Executable files have a variety of different file extensions such as ".com", ".exe", ".bat", ".cmd", ".vbs". These types of files may not be downloaded from the Internet without prior approval from Information Systems Department Leadership and/or the Chief Information Officer.

The next level of danger would be found in files that contain Macros, which is code that runs when a document is open. Macros can be found in a multitude of application files, such as Word Documents, Excel Spreadsheets, PowerPoint Presentations, etc. The typical file extensions would include ".doc", ".xls", ".xla", ".ppt", ".rtf". When downloading files of this type, extreme caution should be taken, making sure that it is from a known trusted site.

The safest form of file to be downloaded from the Internet would be files that are considered read-only. An example of this file type would be an Adobe Acrobat document that typically has the ".pdf" extension.

In all cases, when accessing the Internet and/or downloading files, it is required that it is performed from a computer that is running currently approved and up to date anti-virus protection and that all files are thoroughly scanned before use or installation. As a general rule in all cases, know that the site is a trustworthy site and be aware of the type of files that are being downloaded. If there is any doubt as to the validity of the site or the type of file that is being downloaded, contact the Information Services Department.

Distributing Data and Files

Distribution of Protected Health Information in a non-encrypted manner is prohibited.

The online distribution of business related data and files must be approved by a supervisor and coordinated with the Information Technology Department. This does not include internet email which is addressed in Policy #103.0.15. Distribution of Protected Health Information (PHI) in a non-encrypted manner is a HIPAA violation that could result in fines for Regional West Health Services and possible termination for yourself.

Student Professionalism

The student uses the Internet as an agent of Regional West Medical Center School of

Radiologic Technology and must therefore maintain the highest degree of professionalism at all times. All communications with external organizations must constantly demonstrate this professionalism. Students of Regional West Medical Center School of Radiologic Technology may not visit illegal or pornographic sites, nor distribute illegal or pornographic material.

Sexually related, derogatory or racially intolerant web sites and material is forbidden. Participation in non-business or non-school related chat rooms or bulletin boards is prohibited. These types of sites may be blocked with system tools.

Integrity

Students may not use the hospital's access to the Internet for personal entertainment, information, or financial gain. Use of the Internet for soliciting money or for advocating a religious or political cause is strictly forbidden. The use of abusive, vulgar, or objectionable language on the Internet is unacceptable.

Lawfulness

It is not acceptable to use hospital networking services, resources or facilities for any purposes that violate existing state or federal laws, regulations, policies or procedures. Illegal usage will become the responsibility of the hospital and will lead to disciplinary actions against the student.

Failure to Follow Policy

The hospital monitors and audits all Internet accesses, including both student and guest services for the purpose of assuring system security, proper usage, and for performance impact. The student has no right of privacy in his or her use of Regional West Medical Center Internet services.

Failure to follow the Internet Usage Policy will lead to a student's discipline, which may include reprimand, loss of Internet access, suspension, termination from the Program or legal prosecution.

Stephanie Cannon
Digitally signed by Stephanie Cannon
Date: 2021.12.17 09:47:35 -07'00'

Signature
Stephanie Cannon, MSRS, RT(R)(ARRT)
Program Director

Joshua T. Lively
Digitally signed by Joshua T. Lively
Date: 2021.12.18 07:55:27 -07'00'

Signature
Joshua Lively, MHA, BSRT(R), RT (R)(VI)(ARRT)
Director of Imaging Services

Reference: RWHS Policy 103.0.13

Reviewed: 7/2011, 4/26/12, 2/7/14, 1/23/15, 1/15/16, 1/13/17, 1/17/19, 4/2/20, 9/23/21
Revised: 2/21/13, 1/12/18