MUSKOKA ALGONQUIN HEALTHCARE		**Policy/Procedure Name:**	**Internet Usage by Guest**
Manual:	Administration	**Number:**	
Section:	Risk Management	**Effective Date:**	05 Dec 2012
Pages:	1 of 3	**Revision Date:**	09 Jul 2018

Purpose

The purpose of this policy is to define the appropriate uses of the Internet by patients, guests and visitors at Muskoka Algonquin Healthcare (MAHC).

Scope

The policy pertains to all patients, guests and visitors at Muskoka Algonquin Healthcare (MAHC).

Policy

The Internet may be available at each site of Muskoka Algonquin Healthcare. MAHC provides Internet access to patients, guests and visitors as a courtesy.

MAHC reserves the right to monitor all media and communication technologies within the hospital, including Internet usage. MAHC also reserves the right to restrict access to material on the Internet where the information security officer deems appropriate. An absence of such restrictions does not imply that any information available for access is authorized. Any exceptions must be approved, in advance, by the information security officer.

Internet Usage

Users using the guest Internet access do so at their own risk and will not hold MAHC liable for any associated actions that stem directly or indirectly from using the provided service.

Use of this service constitutes consent. Information disclosure will be used appropriately as permitted and required by law. All employees, contractors, consultants, temporary, volunteers and other workers at MAHC must use the approved corporate information technology resources and may not use public Internet access for business purposes. Guest Internet access may not be used to circumvent existing controls or policies.

MAHC provides no guarantees about the level or availability of service. At no point may a guest, visitor, patient, or any external party connect to the MAHC corporate network. Guest access is provided by clearly labelled wireless access area or wired network jacks.

Each user will maintain one single connection, at most, to MAHC's guest Internet access.

Internet access speeds may be regulated to ensure an acceptable level of usage for a large number of users. This may have an impact on streaming audio/video, web conferencing, online gaming, and overall access.

Users are prohibited from transmitting or accessing any pornographic, threatening, harmful, abusive, harassing, defamatory, libellous, vulgar, obscene, profane, hateful, racially, ethnically or otherwise objectionable material. MAHC will filter sites and services deemed as such to the best of its ability.

Patients and guests are responsible to ensure that information obtained from the Internet must comply with copyright and licensing restrictions in accordance with the publisher/vendor.

MAHC may scan files downloaded from the Internet (software or data) for viruses before provided to the user. Files that are considered harmful will be blocked.
Data obtained through the Internet may not be accurate. The user is responsible for checking the accuracy, adequacy or completeness of any such information.

The Hospital cannot guarantee the security of information transmitted on the Internet. Web conferencing software and hardware is permitted as long it is used for personal communications. Care must be taken so that Hospital staff, patients, and visitors cannot be discerned unless individual consent has been obtained. The associated devices must be turned off when the guest is not using them. The use of peer to peer file sharing applications is prohibited due to their significant drain on network resources.

The illegal or unauthorized access to external resources is strictly prohibited. This includes usage that is not permitted as per the terms and conditions of the external provider. It is the responsibility of the user to understand the acceptable use of any third party service.

The use of the Internet connectivity by guests must not harm the organization in any manner. This includes the use of the MAHC Guest Internet Service for spamming, denial of service attacks and propagation of material contrary to Canadian law. MAHC monitors and audits usage.

In situations where the Hospital provides the guest with a computer for Internet access, the guest is not to modify the computer in any way from its original configuration.

Workstations may be reconfigured on a regular basis and any data stored on these guest systems may be deleted. MAHC monitors and manages guest workstations to ensure their reliability and security.

Guests are strongly advised not to store any confidential data on MAHC supplied computers. Users should be aware that data and files may be deleted at any point and that may be inadvertently made available to other users in the case of MAHC supplied workstations.

Breaches of Policy

MAHC maintains monitoring tools and activity logs to track usage patterns and to ensure policy compliance.

Any instances of inappropriate use should be reported immediately to the area nurse manager or reception desk.

A breach of MAHC policy will result in loss of privileges to further use of the Internet and could result in legal action by MAHC.