General Practice Information Technology (GPIT) Group

Policy on Acceptable Usage of the Internet

File name: GPIT_Internet_Usage_v0_3.pdf
Version number: 0.3
Date: 9/1/2008
Status: final document

Acknowledgement

Request For Comments

This document describes a policy for Acceptable Usage of the Internet in Irish general practice. We would like to hear your opinions. The GPIT Group is happy to have comments, corrections and feedback on this document.

Please write, fax or email your comments to:

       Dr Brian O'Mahony
       GPIT Project Manager
       Convent Road, Lismore
       County Waterford, Ireland
       Phone 058 54255, Fax: 058 53474
       Email bom@iol.ie

If possible, please indicate the document version number, section and paragraph you are commenting on and propose new wording.

Thank you.

GPIT Project Manager
       Dr Brian O'Mahony
GPIT Co-ordinator
       Dr Brian Meade
GPIT Facilitators
       Dr Donal Buckley: HSE Dublin / Mid Lenister
       Dr Fergus McKeagney: HSE Dublin / Mid Lenister
       Dr John Cox: HSE Southern Area
       Dr Frank Hill: HSE Southern Area
       Dr Kieran Murphy: HSE Southern Area
       Dr Anne Lynott: HSE Dublin / North East
       Dr Jack MacCarthy: HSE Western Area
       Dr Barry O'Donovan: HSE Western Area
       Dr John Sweeney: HSE Western Area
       Dr Martin White: HSE Dublin / North East

1 Introduction

1.1. Policy Objective

1.1.1. The objective of this policy is to ensure that the internet facilities provided in general practices are used appropriately and only in connection with official duties.

1.2. Scope

1.2.1. This policy applies to: -

all internet services provided in general practices;

all users, holders and uses of practice internet services.

2 Monitoring of Internet Usage by the practice

2.1. Internet Monitoring

2.1.1. Internet services are provided by the practice to authorised employees, authorised trainee general practitioners, authorised students / work placement staff, and in some cases authorised third parties, for use in connection with official duties only. All internet activities are tracked and logged automatically.

2.1.2. The internet usage records of each user shall be accessible by the practice manager or general practitioners. Practice managers will not routinely monitor individual users use of the internet, but have the right to access the internet history logs of individual users in order to deal with routine work-related matters – e.g. during periods of an employee's leave.

2.1.3. Practice managers or general practitioners will respect the privacy of users when accessing internet history logs and will not access items of a personal nature unless there are compelling conditions that warrant doing so. (An example of a compelling condition would be the detection and prevention of fraud.)

2.1.4. While the practice does not routinely inspect users internet history logs, it does reserve the right to do so: -

    a.   for technical reasons associated with tracing and remedying technical faults and improving performance;

    b.   when required by and consistent with law, and

    c.   when there is reason to believe that violations of the law or of practice policy may have taken place.

3   Internet Usage

3.1.   Acceptable Usage

3.1.1.   Internet facilities provided by the practice may only be used for official purposes in connection with work. This includes using it for training, educational, or research purposes, provided that this is associated with work-related activities or tasks.

3.1.2.   While the practice does not routinely provide internet facilities for third parties – e.g. medical students or students on work placements - if it does so then such services must only be used in accordance with this Policy.

3.2.   Unacceptable Usage

3.2.1.   The practice's internet facilities may <u>not</u> be used: -

    a.   for unofficial or personal purposes, even outside normal working hours;

    b.   to transmit private or confidential information outside the practice, unless it is appropriate to do so and the necessary facilities are in place to protect such information in transit;

    c.   to knowingly misrepresent the general practitioners or practice;

    d.   to enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required)

    e.   to retrieve, create, host or transmit offensive or obscene material, which would cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs, or would bring the practice into disrepute;

    f.   to retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others;

    g.   to retrieve, create, host or transmit material which is defamatory;

    h.   for any activity that would infringe intellectual property rights (e.g. software piracy);

    i.   for any activity that would compromise the privacy of others;

    j.   for any activity that would waste the practice's resources (e.g. staff time and I.T. equipment and networks)

    k.   for any activity that would compromise the security of the practice's I.T. facilities, including confidentiality and integrity of the patient information and availability of I.T. services (e.g. by carelessly causing computer virus infection)

    l.   for any activity that is illegal.

3.2.2.   Only internet facilities provided by the practice may be used in connection with private and or confidential information.

3.2.3.   Internet facilities may only be used by users to whom the practice has directly provided these facilities. Users may not use other users' internet facilities.

4 Internet Security

4.1. Internet Privacy & Confidentiality

4.1.1. Confidential information must <u>not</u> be transmitted via the public internet. In special circumstances it may be possible to provide additional security measures to enable such transmission outside the practice and it is only in these circumstances that it will be permitted.

4.1.2. It is acceptable to exchange information with services such as HealthLink or other health care messaging implementations, Heartwatch and the Primary Care Reimbursement Service. These sites are designed to authenticate users and exchange information securely.

5 Roles & Responsibilities

5.1. Internet Users' Responsibilities

5.1.1. Each user of the practice's internet facilities is responsible for: -

    a. complying with the policy contained herein this document;

    b. complying with instructions issued by the practice manager or general practitioners;

    c. attending appropriate training courses, as provided or arranged by the practice, so that he/she is aware of the proper use of the internet;

    d. the data downloaded or uploaded via their use of the internet;

    e. the privacy of his/her password(s) and other similar confidential authentication information;

6 Breach of this Policy

6.1. Breach of Policy

6.1.1. The general practitioner reserves the right to take such action as he or she deems appropriate against users who violate the conditions of this Policy. Such violations will be regarded as a disciplinary matter for staff. For non practice Staff action will be taken in conjunction with their educational institution, employer, or relevant authority.

6.1.2. The practice may withdraw computer systems facilities from any computer user who it believes is not complying with this Policy or who misuses computer systems in any manner.

6.1.3. The use of computer systems for illegal activities by any computer user is a breach of this Policy and may result in prosecution. The practice will not afford any protection to employees or others who engage in such activities and will co-operate fully with, and provide whatever information may be required, to facilitate investigations into such activities.

7 Staff Acceptance

7.1. Signatures

I confirm that I have read and understood this practice internet usage policy and accept its terms and conditions.

PRINT NAME	Signature	Date