INTERNET AND EMAIL MONITORING, ADMINISTRATION AND REPORTING PROTOCOL

Reference No:	UHB 048	**Version No:**	UHB 1	**Previous UHB / LHB Ref No:**	N/A

Documents to read alongside this Protocol	IT Security Policy, Appendix 5 (Internet/Email Policy)

Classification of document: IT

Area for Circulation: IT Security Office

Author: IM&T Security Manager

Executive Lead: Director of Innovation and Improvement

Group Consulted Via/ Committee: IT Security Forum, HR

Ratified by: Information Governance Committee

Date Published: 26th May 2011

Version Number	Date of Review	Reviewer Name	Completed Action	Approved By	Date Approved	New Review Date
UHB 1				Information and Governance Committee	26/04/2011	01/01/ 2014

Disclaimer

When using this document please ensure that the version you are using is the most up to date either by checking on the UHB database for any new versions. If the review date has passed please contact the author.

OUT OF DATE POLICY DOCUMENTS MUST NOT BE RELIED ON

CONTENTS **Page No.**

Level of competency

This protocol assumes that the person using the monitoring software (Mail Marshal and WebMarshal) has the skills and working knowledge at the depth and scope required in order to carry out the requirements of this protocol.

Purpose

The UHB offers staff both business and limited personal use of email and internet services however, email and internet access has the potential of presenting the UHB with real and growing problems related to inappropriate use of email and web browsing.

The purpose of this document is to establish an effective protocol for the administration of monitoring and reporting inappropriate use. The protocol will legitimise and protect the actions of the IM&T Security Manager, Data Protection Manager and other senior IM&T Staff when reporting inappropriate use of these services.

Policy on Staff Monitoring

The IM&T Security Manager is responsible for monitoring staff use of Internet and Email to ensure compliance with the UHB's Internet/Email Policy. Monitoring is also carried out by the Data Protection Manager and the IM&T Security Office, Project Support Officer. All staff are made aware of the UHB's intent to monitor and are required to sign the User Compliance Declaration statement found on the UHB's IT User Security form.

The IM&T Security Manager will produced regular reminders of the Internet/Email Policy and the UHB's Internet and Email monitoring capabilities which are distributed via the UHB's email Administrator and Intranet News page.

There are three legal developments which relate to employers monitoring staff access:

- The Regulation of Investigatory Powers Act (RIPA), which came into force in October 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (The Regulations);

- The Data Protection Act 1998;

- The Human Rights Act 1998.

Regulation of Investigatory Powers Act

Under RIPA, it is a criminal offence to intercept communications (such as emails and telephone calls) being transmitted on, from or to a private telecommunications system (such as that operated by an employer) without consent from the sender and recipient. The Lawful Business Practice Regulations lay down exceptional cases where interception without consent is allowed. The main exceptions relevant to employers are as follows:

- Establishing the existence of facts;
- Ascertaining compliance with regulatory and self-regulatory practices;
- Ascertaining employees' performance if the system is used to perform duties;
- Prevention and/or detection of crime;
- Investigating whether there is an authorised use by the employee;
- Ensuring the effective operation of the IT system.

However, there is still an obligation on the employer to make "all reasonable efforts" to inform the employees who use the system that all Internet and email use is monitored. This is accomplished via the Internet/Email Policy and when staff sign an IT User Security Form when applying for a Network account.

Information Commissioner's Code of Practice

Employee monitoring will be subject to the provisions of the Data Protection Act 1998 (DPA). Key provisions of the Information Commissioner's Employment Practices Code that provides guidance on monitoring staff are as follows:

- Set out clearly to workers the circumstances in which they may or may not use the employer's internet and email system for personal communication.
- Keep to a minimum those who have access to personal information obtained through monitoring. Subject them to confidentiality and security requirements and ensure that they are properly trained where the nature of the information requires this.
- Do not use personal information collected through monitoring for purposes other than those for which the monitoring was introduced unless:
    - It is clearly in the individual's interest to do so; or

  - It reveals activity that no employer could reasonably be expected to ignore.

- Inform workers of the extent to which information about their internet access and email is retained in the system and for how long.

- Wherever possible avoid opening emails, especially ones that clearly show they are personal.

The Human Rights Act

Under Article 8 of the European Convention of Human Rights an employee has the right to respect for private and family life, his home and his correspondence. This has implications for employee monitoring.

The main principle in employee monitoring is that it is **proportionate to its aim.** The UHB's Internet/Email policy ensures that staff are made aware that their use of the Internet and Email will be monitored and only actions which do not comply with the policy will be reported.

Types of Dangers Arising from Internet and Email use

- Pornographic/Inappropriate material
- Disclosure of Patient Identifiable Data
- Infringement of copyright
- Legally binding agreements
- Computer Viruses/Malicious Software
- Bullying and Harassment (Dignity at Work)
- Breaches of Confidentiality
- Bringing the UHB into disrepute

Administration of Monitoring

Folders will be created in the IT Security email inbox by the IM&T Security Manager or Data Protection Manager. Folders are only accessible by IM&T Security Office staff. These folders will store copies of emails sent or received by UHB staff that contravene the UHB's Internet/Email Policy; they will also store copies of warnings sent to UHB staff regarding unacceptable use of the UHB's email system.

Folders will also store emails sent by WebMarshal regarding possible inappropriate web browsing and copies of warnings sent to UHB staff regarding unacceptable use of the Internet.

The content of folders will be regularly reviewed by the IM&T Security Manager or Data Protection Manager. If there are no further occurrences of the issue that caused an email (from MailMarshal or WebMarshal) to be copied into a folder, after 12 months, the email will be deleted. Further occurrences may lead to the Reporting Process (page 8) being followed.

Email Monitoring Software (MailMarshal) Configuration

The MailMarshal monitoring software is hosted by Health Solutions Wales (HSW) on an All Wales basis. IM&T Security Office staff log-into the software via the Digital All Wales Network 2.
MailMarshal is configured locally to quarantine all emails which contain the following content:

- Offensive/Profane language
- Racial language
- Sexual language
- Encrypted files
- Executable files
- Chain emails
- Images containing 'flesh tones'
- Video/Sound files

Sent/received emails that breach the Internet/Email Policy

Emails sent to and from a UHB email account are quarantined by MailMarshal where they do not satisfy some or all of the parameters programmed into the system. Quarantined emails are regularly reviewed by the IM&T Security Office and released if they are business related. Emails are quarantined by MailMarshal under the following headings; Encrypted, Executables, Video and Sound, Junk, Language, Suspect Images.

Encrypted

Emails containing encrypted or password protected content are quarantined by MailMarshal. Encrypted business related email will be released. Password protected content (which is not secure and as such not permitted) containing patient identifiable data (PID) will be dealt with as follows. Where the email is sent into the UHB from outside NHS Wales, the UHB member of staff will be reminded (by email from the IM&T Security Office) of UHB policy and requested to advise the sender not to send PID by email. If a UHB member of staff sends an email to a non-wales.nhs.uk address they will be reminded of UHB policy and advised that if they send further emails containing PID they will be reported (see Reporting Process, PID). The email will not be released from quarantine.

Executables
These are emails that contain files to be downloaded to a programme on the recipient's computer, with the intention of installing software, modifying or carrying out some action within that programme. The UHB IT Security Policy requires that the IM&T Security Manager authorises this. There is an exception to this regarding executable files downloaded by technical staff within the IM&T Department for business purposes. Staff sending or receiving executable files must explain their purpose to the IM&T Security Manager.

Video and Sound
Any email containing a video or sound file is automatically quarantined by MailMarshal. The sender and recipient are automatically informed by MailMarshal (by email) that the email has been quarantined and that if it is a personal email it will not be delivered. In the first instance (unless the content is inappropriate) UHB staff will be sent a copy of the Do's and Don'ts (see Reporting Process).

Junk
Emails are quarantined if the email is a 'chain email' (see Definitions in the Internet/Email Policy). The sender and recipient of chain emails are automatically informed by MailMarshal (by email) that the email has been quarantined and that if it is a personal email it will not be delivered. In the first instance (unless the content is inappropriate) UHB staff will be sent a copy of the Do's and Don'ts (see Reporting Process).

Language
MailMarshal has a built-in 'language censor that will quarantine emails containing offensive, profane, sexual or racial language. More detail of unacceptable content is contained in the Internet/Email Policy. The IM&T Security Office will make a decision on the acceptability of language used in an email and either release the email or, in the first instance (unless the content is inappropriate) UHB staff will be sent a copy of the Do's and Don'ts (see Reporting Process). Where emails are sent to the UHB, containing unacceptable language, the recipient will be told to advise the sender of UHB Policy regarding acceptable email content (see Reporting Process, Inappropriate content from outside the UHB).

Suspect Images
Any email containing an image that has 'flesh tones' in it will be quarantined under this heading. The sender and recipient are automatically informed by MailMarshal (by email) that the email has been quarantined and that if it is a personal email it will not be delivered; if the email is business related it will be released. In the first instance (unless the content is inappropriate) UHB staff will be sent a copy of the Do's and Don'ts (see Reporting Process).

Non-Inappropriate content
An example of non-inappropriate images would be wedding photos, baby photos (appropriately dressed) or pictures of pets. The infrequent use of 'mild' profanity, used in a non sexual way is deemed to be non-inappropriate.

Inappropriate Content
Inappropriate use is defined in the Internet/Email Policy. Examples of inappropriate email content are; full frontal nudity, any depiction of a sex act, extreme profanity, any racial and/or hate content, images of children that are not pornographic but that indicate, by the nature/composition of the image, there may be child protection issues.

Patient Identifiable Data (PID)
If PID is identified in any quarantined email, the procedure detailed in 'Encrypted' above will be followed.

Spam
Spam email is managed on an All Wales basis by HSW; they are responsible for preventing Spam emails reaching the UHB. The IM&T Security Office is able (by requesting Configurator time with HSW) to include the email address of Spam emails that reach the UHB into the centralised Spam filter. The IM&T Security Office does not have direct access to the Spam filter and as such cannot search the filter for an expected email that may have been quarantined as Spam.

Emails with 'Personal' in the subject line
Where emails with 'Personal' in the subject line are quarantined by MailMarshal they will not opened by the IM&T Security Office. Stage 1 of the 'Reporting Process, Content is not Inappropriate' will be followed. The email will not be released from quarantine.

Due to the design of MailMarshal, in some instances emails marked personal can be inadvertently opened by the system and the emails content viewed. Where this happens and content viewed constitutes a serious breach of any UHB Policy, or the content is such that it cannot be ignored; the matter will be referred to the Technical Development, Network and Support Manager for advice regarding reporting the email sender (unless doing so would breach any legislative requirements).

Reports
If the IM&T Security Manager or Data Protection Manager suspects, from viewing information in MailMarshal, that the UHB's Internet/Email Policy has, or possibly has been contravened (for example excessive personal use), a report may be generated. If there is evidence that a member of staff has contravened the Internet/Email Policy (or any other UHB Policy), the relevant Reporting Process will be followed. If a manager requests a report on a member of their staff the request must be supported by HR. Currently, there are limited reporting capabilities in MailMarshal.

Reporting Process
The role of the IM&T Security Office in monitoring Internet and Email use is to decide (in their opinion) if an email breaches the UHB Internet/Email Policy (or any other UHB Policy) and if it does, to report this to the member of staff's manager (or the Medical Director for clinicians) and HR. The reporting process is detailed below.

Patient Identifiable Data
Where it is identified that a member of staff has previously been reminded of UHB policy regarding sending PID by email outside NHS Wales; the Report Log (appendix 1) will be completed and the member of staff's manager and HR informed. If the member of staff is a clinician, the Medical Director and HR will be informed. A copy of the email will be retained in a secure folder, pending any investigation.

Content is not Inappropriate
Stage 1 - Where a quarantined email has content not permitted by the UHB Internet/Email Policy; in the first instance the member of staff will be sent an email from the IM&T Security Office reminding them that the content is not permitted. This email will also contain a copy of the 'Do's and Don'ts' for guidance (appendix 2). A copy of the email will be kept in a Folder (see Administration of Monitoring).

Stage 2 - If a subsequent email is quarantined by MailMarshal within 12 months of the first one, the member of staff will be sent an email that includes a copy of the first email and warns them that should they send another email that breaches UHB Policy, their manager and HR will be informed and this may lead to disciplinary action.

Stage 3 - If a subsequent email is quarantined by MailMarshal within 12 months of the second warning email; a Report Log will be completed and the member of staff's manager and HR informed. The IM&T Security Office will produce copies of emails, the Report Log and any other relevant documents to the manager, HR and (if relevant) an appointed Investigating Officer.

Content is Inappropriate
Where a quarantined email has content that is considered (by the IM&T Security Office) to be inappropriate a Report Log will be completed and the member of staff's manager and HR informed. IM&T Security staff will produce copies of emails, the Report Log and any other relevant documents to the manager, HR and (if relevant) an appointed Investigating Officer.

Where it is not clear as to whether or not email content is inappropriate, advice will initially be sought from the Technical Development, Network and Support Manager. Subsequently, advice may be sought from HR.

Inappropriate content from outside the UHB
Where emails with inappropriate content are sent to UHB staff from outside the UHB; the member of staff will be sent an email by the IM&T Security Office instructing them to inform the sender not to send such emails and that if they continue, their email address will be 'blacklisted'. This will prevent them from sending further emails to the UHB. A copy of emails sent by the IM&T Security Office will be kept in a Folder.

Child or Extreme Pornography
Should monitoring reveal material of a criminal nature such as child pornography or extreme pornography (Criminal Justice and Immigration Act 2008, section 63) the police will be informed immediately. The Director of Workforce and Organisational Development and Head of IT will be informed but not shown the content of the email as legislation does not permit this.

Internet Monitoring Software (WebMarshal) Configuration

WebMarshal monitoring software is managed locally on the UHB's Network and is configured to produce scheduled reports on access to inappropriate sites using the following categories

- Adult
- Chat
- Drug
- Gambling
- Video and Sound
- FTP
- Hate
- Nudity
- Sexually Explicit
- Violence/Profanity
- From time to time other categories may be added

Blocked Web Sites
WebMarshal is configured to prevent access to a number of categories of web site (e.g. adult sites, gambling, audio/video, social networking) in line with the UHB's Internet/Email Policy. Where a member of staff attempts to browse a web site that is not permitted by the Policy, WebMarshal will block access to the site and display a message on the member of staff's computer screen informing of the reason why the site has been blocked. WebMarshal will also send a notification email to the IM&T Security Office, informing of the attempted access.

Inappropriate Internet Browsing
It is not always clear from the WebMarshal email notifications, whether or not the attempted access to an inappropriate web site was accidental, deliberate or caused by web pages being 'hijacked' and the user re-directed to an inappropriate site. Where it is suspected that access may be deliberate, the WebMarshal email notification will be copied to a Folder. Subsequent WebMarshal email notifications may lead to the Reporting Process (page 11) being followed.

Proxy Sites
Proxy sites (web sites that allow users to by-pass Internet monitoring) pose a security threat to the UHB network. Were WebMarshal email notifications report an attempted access to a proxy site, the member of staff will be sent an

email informing them of UHB policy and advising that further occurrences will be reported to their line manager and HR. A copy of the email sent to the member of staff will be copied to a Folder. Further occurrences may lead to the Reporting Process being followed.

Reports
If the IM&T Security Manager or Data Protection Manager suspects, from viewing information in WebMarshal, that the UHB's Internet/Email Policy has, or possibly has been contravened, a report will be generated. If there is evidence that a member of staff has contravened the Internet/Email Policy (or any other UHB Policy), the Reporting Process will be followed.

Reports on a member of staff's Internet browsing can be requested by their manager (supported by HR) or by HR. A request must detail the scope of what is to be reported. Requests must be in writing (email counts) to the IM&T Security Manager, or in his absence to the Data Protection Manager. Reports are available for up to 90 days prior to the request.

Reporting Process

Suspected Inappropriate Browsing
Where evidence from WebMarshal email notifications or reports generated by the IM&T Security Manager or Data Protection Manager suggest that, on the balance of probabilities, a deliberate attempt to browse web sites not permitted by the Internet/Email Policy have been made, a Report Log (appendix 1) will be completed. Details of the member of staff's web browsing will be reported to their manager and HR. The IM&T Security Office will produce copies of WebMarshal notification emails, the Report Log and any other relevant documents to the manager, HR and (if relevant) an appointed Investigating Officer.

Where it is not clear as to whether or not the web browsing is inappropriate, advice will initially be sought from the Technical Development, Network and Support Manager. Subsequently, advice may be sought from HR.

Examination of Computers
In some circumstances it may be necessary to examine a member of staff's computer. Only in the most severe cases will it be necessary to remove IT equipment. If a serious misuse has been suspected such as the browsing of child or extreme pornography the equipment must be preserved as evidence. The equipment must be disconnected from the electricity supply, immediately removed and secured at the IM&T Security Office. Any examination must be performed by the IM&T Security Manager plus one other senior IM&T staff member. This examination can only be performed on authorisation of the Technical Development, Network and Support Manager or Head of IT. If evidence of child or extreme pornography is found the investigation must stop and the findings reported to the Police, Head of IT and the Director of Workforce and Organisational Development. Making a back up copy of any content or showing the material to anybody other than the Police may

compromise the investigating managers and any subsequent police investigation and therefore is not permitted.

Equality Statement

We have undertaken an Equality Impact Assessment and received feedback on this protocol and the way it operates. We wanted to know of any possible or actual impact that this protocol may have on any groups in respect of gender, race, disability, sexual orientation, Welsh language, religion or belief, transgender, age or other protected characteristics. The assessment found that there was no impact to the equality groups mentioned. Where appropriate we have taken the necessary actions required to minimise any stated impact to ensure that we meet our responsibilities under the equalities legislation.

Appendix 1

INTERNET / EMAIL REPORT LOG

Date -	**WebMarshal / MailMarshal** (delete)

Name of Individual – **Department** – **Location** -	**Log-in Name** – **PC ID** – **Account Authorised by** -

Report Commissioned By (name)**:** **IM&T Security** – **Subject's Manager** – **HR** -	**Scope of Report** -

IM&T Security Office Actions: 1 - 2 - 3 - 4 - 5 - 6 - 7 -

IM&T Security Office Findings: 1 - 2 - 3 - 4 -

Advice sought (where deemed necessary**) from:**

Name –	**Name** –
Position -	**Position** -

Evidence Attached:	
IT Security Form -	**X**
Copy of Quarantined Email -	**X**
Evidence From MailMarshal -	**X**
Evidence From WebMarshal -	**X**

Reported To:

Subjects Manager –	**HR** –
Date –	**Date** -

Further Reporting (details)

IM&T Security Office:
Name –
Position –
Date –

APPENDIX 2

ALL INTERNET + EMAIL USERS MUST READ THIS

The UHB's Internet/Email Policy has been reviewed. All staff are advised to familiarise themselves with this policy, particularly the conditions governing personal use.
This is available from; the UHB Intranet – IT Security and Confidentiality – Key Documents – IT Security – Appendix 5 of the IT Security Policy.

THE KEY POINTS ARE:

All Internet and email use is monitored and recorded.

INTERNET	EMAIL
• Personal use is restricted to non-core hours (including break times). • Adult sites, hate sites and sites that link to, or allow you to gamble/bet are blocked. • Sites that have downloadable video content (e.g. you tube, video Google, mp3) are blocked. • Social networking sites are blocked. • Streaming media sites (e.g. radio stations) are blocked. • eBay is blocked, apart from registered (with the IM&T Security Manager) users for UHB business purposes. • Software must not be downloaded from the Internet without permission from the IM&T Security Manager. Screensavers, smiley's, animated emoticons etc. are not permitted to be downloaded.	• Personal use is restricted to non-core hours (including break times) and a maximum of 25 emails/day. • Personal emails should be marked 'Personal' in the subject line. • Personal videos, sound files or pictures are not permitted and will not be delivered. (policy – limited personal use definitions) • Chain emails that encourage the recipient to forward to others are not permitted and will not be delivered. • Personal emails addressed to 20+ recipients will not be delivered. • Emails containing unacceptable content (see policy) will be reported to line managers and HR. • Business and personal content should not be included in the same email.

For further advice and guidance on the permissible use of Internet or Email, please contact the IM&T Security Office, Tel: 2074 6677; Fax: 2074 5626
Email: cv.imt.security@wales.nhs.uk