Reference Number: UHB 426 **Version Number:** 1.1	**Date of Next Review:** 8th Aug 2020 **Previous Trust/LHB Reference Number:** N/A

INFORMATION TECHNOLOGY E-MAIL LOCAL PROCEDURE

Introduction and Aim

This document is written in support of the Information Technology (IT) Security Policy and the NHS Wales All Wales Email Use Policy. It provides a mechanism to achieve and maintain appropriate security arrangements in respect of Cardiff and Vale University Health Board's (UHB) IT systems that hold confidential and sensitive patient and business information.

The IT Security procedures of the UHB are to ensure the safety and security of all UHB IT systems, software and in particular the UHB's Network so as to produce a safe and secure environment in line with NHS and statutory policies and procedures. This document provides further information as to the detail of the policy and its supporting information.

Objectives

- Successful implementation of this procedure will address business and performance standards for example the requirement to meet Caldicott standards, Health and Care Standards (2015)
- Aspire to meeting BS7799/ISO27001 standards and the Information Governance Toolkit Standards as far as possible in the Welsh context.

Scope

This procedure applies to all of our staff in all locations including those with honorary contracts

Equality Impact Assessment	An Equality Impact Assessment has been completed for the overarching IG and IT Policies. The assessment found that there was some impact on the equality groups mentioned in relation to communication. An action plan has been developed to address those areas.
Health Impact Assessment	A Health Impact Assessment (HIA) has not been completed. Not Required.
Documents to read alongside this Procedure	Information Governance Policy Information Technology Security Policy Information Risk Management Procedure A Guide to Incident Reporting NHS Wales All Wales Email Use Policy Data Protection Policy
Approved by	Information Governance Sub Committee

Accountable Executive or Clinical Board Director	
Author(s)	Richard Williams (IT Security) Ann Morgan (Information Governance)

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments

Version Number	Date of Review Approved	Date Published	Summary of Amendments
1	08/08/17	28/08/18	New Procedure
1.1	08/08/17	28/08/18	Admin changes to reflect current contact details

Contents Page

1 Introduction

It is essential that all information systems in the Cardiff and Vale University Health Board (the UHB) are protected to an adequate level from events that may jeopardise health care activities. These events may include accidents as well as behaviour deliberately designed to cause difficulties.

This procedure supports and should be read in conjunction with the NHS Wales All Wales Email Use Policy (the Policy).

The use of the UHB email facility is controlled and monitored to: -

- Ensure effective communication
- Encourage best practice
- Maximise efficiency
- Prevent misuse
- Protect employees from any kind of harassment
- Minimise the organisation's liability arising from inappropriate use of the email facility

This procedure complies with the following references: -

- NHS Wales All Wales Email Use Policy
- Data Protection Act 1998
- Human Rights Act 1998
- Common Law as it relates to confidentiality
- The Caldicott Report requirements
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- The Telecommunication (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Equality Act 2010
- The Computer Misuse Act 1990
- ISO27001 Information Security Standard

2 Responsibilities

The following areas of responsibility have been defined:

IM&T IT Services
The IT Services Department are responsible for the email system control, support and individual email accounts management.

Refer to appendix A for useful contact information.

Information Governance (IG)
The IG Department manage the day-to-day monitoring functions of the Mail Marshal Security Monitoring system.

Refer to appendix A for useful contact information.

All Users
All UHB users who have been given access to the UHB email system have to remain diligent and vigilant at all times when communicating any information by email on behalf of the UHB.

In particular, users must think carefully when sending Patient Identifiable Data (PID) and Personal Identifiable Information (PII):

- Does the information need to be sent via email?
- Do you need to send copies (c.c) of the email?
- Consider the content of the email, how much information is required.

These decisions must always be balanced against the need to provide safe care. Missing or incomplete information could be dangerous.

Before users send PID/PII email they should check:

Emails containing PID / PII attachments CAN be sent to:	**Emails containing PID / PII attachments CANNOT sent to:**
Recipients within the Health Board	Other NHS email services outside Wales
Recipients within NHS Wales organisations that have emails that end with ‘wales.nhs.uk’, including NHS Wales GP surgery addresses	Voluntary Services
	Any suppliers (e.g. medical gas suppliers etc)
	Personal mailboxes (e.g. Doctors.net, hotmail, yahoo etc)
	Patients

Non Conformance
There is a requirement for all staff to comply with this procedure and the associated Policy, and where requested, to demonstrate such compliance. Failure to comply will be regarded as a disciplinary incident, and will be dealt with under the appropriate UHB’s Human Resources Policy.

3 UHB Management of Email

The IT Services Department are responsible for email system management. Refer to appendix A for useful contact information.

The procedure for management of emails is extensive and varied:

New accounts
An NHS Wales email account will only be issued to a UHB member of staff upon receipt of an application form authorised by his/her line manager and accompanied by a signed declaration of intent to comply with the Policy and this procedure.

Moving accounts
Where a member of staff transfers to another organisation who is part of the National Email Service, his/her email address will be made available to the new employing organisation.

The current email account and its contents will remain the property of CAV UHB.

Closing old accounts
When a member of staff leaves and is not moving to another NHS Wales organisation, his/her email address will be removed from the Global Address List immediately and the user account will be disabled.

Permanent deletion of the user and email account will take place within 28 working days.

Prior to leaving the organisation the staff member should make arrangements to ensure all relevant business related information is transferred from the e-mail account and onto the file server. It is the responsibility of the line-manager of the individual to ensure that this process is completed.

4 UHB Monitoring of Emails

All monitoring of emails by the UHB will be undertaken in line with the Policy, by the Information Governance Department. Refer to appendix A for useful contact information.

Access to Email Messages
The UHB will not normally access any individual's mailbox without the permission of that individual. However, there may be occasions when it is necessary to access email messages without permission. Examples of reasons for accessing an individual's mailbox are: -

- To action subject access requests under the Data Protection Act
- To action Freedom of Information requests
- To obtain evidence in legal proceedings
- To obtain evidence in a criminal investigation

- To action a line of business enquiry
- To obtain evidence in support of disciplinary action
- To activate 'Out of Office', for example, if a user is unexpectedly absent from work.

This list is not definitive.

If either party is involved with a grievance, disciplinary or any other type of investigation, this needs to be highlighted to the IT Security Manager and specified on the on-line form "Access to Email Messages" (see below).

Attempts should be made to avoid accessing emails marked "PERSONAL", unless there is a legal basis to do so. Where in doubt advice should be sought from either Human Resources or the Information Governance Departments.

Where it is not possible to ask the permission from the member of staff whose mailbox needs to be accessed, the procedure for gaining access to their mailbox is:

- The request is submitted by email requesting access to the IT Security Department
- IT Security will authorise access providing; full details are supplied, management confirmation of requirement, and if appropriate whether either party is currently involved with a grievance, disciplinary or any other type of investigation
- Following IT Security approval, access is gained by a qualified member of the IT Services Department
- A record is made of access to the mailbox by both IT Security and IT Services
- Where appropriate inform the person whose mailbox was accessed

Malware protection
All incoming and outgoing email will be automatically monitored for computer viruses. Any suspect email will be impounded and investigated.

5 User Usage of Email

Personal Use
Under the Policy staff are allowed a reasonable amount of personal use of the email facility. When sending a personal email staff must include the word "PERSONAL" (in block capitals) in the Subject field.

Where staff use the email facility for personal use they must create a sub folder within their mailbox called "PERSONAL" (in block capitals). All personal emails (both sent and received) must be moved to this sub folder, and deleted on a regular basis.

Staff should not using their work email address for non-work related on-line subscription services, such as newsletters, promotions and offers. This is to avoid both the potential security risks and the large volumes of email this can generate.

Storage and Retention of Email
All emails should be retained and stored in accordance with local and national records management guidance. Emails and attachments that form part of the business process are business records and must be captured into corporate / health records management systems in electronic and / or paper format. Members of staff are responsible for identifying these records and managing them correctly in accordance with this policy and NHS retention and destruction schedules.

Emails that are not deleted or moved into the relevant records management systems will be automatically stored in a secure data store for a period of 6 years, after which they will be permanently deleted. There may be occasions where access to the data store for the purposes of responding to a Freedom of Information request or an investigation will be made without the authority of the individual and with the specific authority of the Information Governance and/or Human Resources management.

Signatures
Signatures should be used on emails particularly where the content contains personal identifiable information (PII) or patient identifiable data (PID), so that the sender may be contacted if an email is received in error.

Out of Office Auto-Replies
Whenever possible Out of Office auto-replies should be turned on when emails cannot be read for a significant period of time, for example when in a meeting or on annual leave.

As a minimum requirement, Out of Office auto-replies they should:

- Inform the recipient of the reply whether their original email is being dealt with in your absence;
- Details of who to contact if the email is urgent;
- If on leave, the date of your return.

Automated Email Disclaimer
All external email must have a disclaimer clearly stating the email has no contractual obligations or is binding in any way. It must also highlight the status of the information sent in respect of the FOI Act. This disclaimer will be bi-lingual.

The following standard statements will be added automatically by the UHB, therefore individual disclaimers will not be required:-

Confidentiality

Limits to message size

The combined size of the email and its attachments cannot exceed the all Wales agreed standard (currently set at 25 MB). Emails exceeding this size will be blocked and the sender informed.

Advice can be obtained from the IT Helpdesk and further options explored as appropriate.

Compliance with the Welsh Language Scheme

At all times staff must ensure that email messages comply with the requirements of the UHB's Welsh Language Scheme. This means that out of office replies, automatic signatures, etc must be displayed in a bilingual format.

Further advice and guidance can be obtained via the Welsh Language page on the UHB Intranet site.

Use of other people's email accounts
The use of another person's email account is not permitted. If you need to send an email on behalf of another member of staff this must be performed through the delegated access function which ensures that the recipient is informed of both who sent the email and on whose behalf it was sent.

Auto-forwarding
Email must not be auto-forwarded outside of the organisation.

Use of meaningful subject lines
The absence of a meaningful subject line makes it impossible for sender or recipient to safely manage their email folders. *Confidential* emails should include the word in the subject line.

6 User Management of Email

Management of Emails
The written and permanent nature of email messages means that they should be treated as records of business activities. As email can be used for a variety of purposes, email messages are not always treated as records of business activities leading to important records being lost and potentially leading to difficulties in accounting for decisions and actions taken. To ensure that there is a full record for evidential and accountability purposes it is important that everyone in an organisation who uses email for business purposes is aware that email messages might need to be retained with the formal business records and how these email messages should be treated.

It is the responsibility of all members of staff to manage their email messages (received, sent and deleted messages) appropriately. It is important that email messages are managed in order to comply with Data Protection and Freedom of Information legislation. Managing email messages appropriately will also mean that work can be conducted more effectively as it will help towards locating all the information relating to specific areas of business.

To manage email messages appropriately members of staff need to separate email messages that are records of their business activities from ephemeral email messages. It is important that email messages that are records are moved from personal mailboxes and managed with, and in the same way as other records. Email messages which have no longer term significance should be managed within the mailbox and kept only for as long as required before being deleted.

Where emails are used to support a business process a shared role-based email account should be established to ensure that emails can be processed when members of the team are unavailable. The use of role based email accounts should be subject to a formal documented procedure (See Management of Role Based Email Accounts).

Where emails are used to transmit person identifiable information (PII), messages should be copied to the appropriate file server record store and then deleted from email message boxes. The use of email for PII should be subject to a formal documented procedure (See Data Protection Policy)

Management of Role Based Email Accounts

Role based email accounts allow a number of users to read and send messages on behalf of the account owner whilst preserving their individual accountability. They are required wherever email is used to support a business process that requires a guaranteed response to a message. In the simplest form this may simply mean that a manager allows delegated access to his / her email account. In a more formal environment it may involve several members of staff having various levels of read/send permission to have a shared departmental account e.g. ESR Status reports. In all cases, a role based mailbox must have a named owner.

When role based mailboxes are created, there should be a clear definition of the purpose of the mailbox, who will have access to the contents of the mailbox and who is likely to send email messages to the mailbox. The owner of the mailbox needs to decide and communicate to the other users how to treat the email messages that will be received into that mailbox. The owner of the mailbox should consider the following aspects:

- Who should answer which email messages?
- How it can be determined that someone has responded to an email message?
- If someone has replied to an email, should the received email or the reply remain in the mailbox?
- Who has the responsibility to capture the records of the email messages?
- Where will a record of the email messages received and replied to, be maintained?

This document is one of several that sustain the UHB's IT Security Policy and IT Security Procedure.

Useful Contacts

Appendix 1

IM&T IT Security cv.imt.security@wales.nhs.uk

Head of IT and Strategic Planning
Nigel Lewis Nigel.Lewis@wales.nhs.uk
Tel 02920 745600

Technical Development, Network and Support Manager
Gareth Bulpin Gareth.Bulpin@wales.nhs.uk
Tel: 02920 745605

IT Helpdesks
UHW (East) IT.Helpdesk.UHW@wales.nhs.uk
Tel 02920 745073
UHL (West) Llandough.Helpdesk@wales.nhs.uk
Tel 02920 715218

Information Governance cav.ig.dept@wales.nhs.uk
Including Data Protection/Freedom of Information and E-mail monitoring

IG Manager/Clinical Coding
James Webb james.webb@wales.nhs.uk
Tel 02920 746208

Corporate Governance Senior Information and Communication Manager
Ann Morgan ann.morgan4@wales.nhs.uk
Tel 02920 744870

Information Governance Co-ordinator
Denise Gulley denise.gulley@wales.nhs.uk
02920 745625