Reference Number: UHB 422 **Version Number:** 1.1	**Date of Next Review:** 20th Sep 2019 **Previous Trust/LHB Reference Number:** T342

INFORMATION TECHNOLOGY SECURITY
ANTI-VIRUS GUIDANCE

Introduction and Aim

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

The UHB must ensure the safety and security of all its 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 on access control to support the IT Security Policy and its related control documentation.

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 guidance 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.
Documents to read alongside this Procedure	Information Governance Policy Information Technology Security Policy Information Technology Security Procedure Information Risk Management Procedure Electronic Incident Reporting Guide
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	20/09/16	28/08/18	Original Document
1.1	20/09/16	28/08/18	Review and updated to new guidance document in line with the Schedule of Revision approved by IGSC. Admin changes to reflect current contact details

Contents Page

1 Introduction

The increasing number of staff who have access to networked PCs, laptops and devices has made it difficult for the Cardiff and Vale University Health Board (the UHB) IM&T Department to police the activities of all users at all times.

There is a very real risk of infection by a virus is whenever files are transferred onto a computer from any external source; e.g. data transfers by CD/DVD, memory sticks, a file contained within an e-mail or a file downloaded from the internet.

It is undoubtedly the case that the growth of internet use will greatly increase the exposure to a wider variety of viruses.

The objective of the UHB's Anti-Virus Guidance is to ensure that all staff are made aware of the dangers that can be caused by viruses and to make staff fully aware of the potential impact that their action can have on the whole of the IT Network in an attempt to ensure that any possible risks can be minimised.

2 Responsibilities

All users of the UHB's IT network have the following personal responsibilities.

All staff must:

- Use Common Sense and treat with caution any e-mail that appear to come from senders who are unknown to them
- Make every possible effort to ensure that they do not introduce viruses.
- Report **immediately** any virus infection activation by completing an e-Datix Incident Report and e-mail the IT Security Manager at CV.IMT.SECURITY@WALES.NHS.UK
- Be vigilant and take care when receiving any electronic information from an unknown source, this will include such items as attachments within E-mail or World Wide Web Hyperlinks
- In exceptional circumstances if situations arise that require staff to access information from a questionable/unknown source, guidance **MUST** always be obtained from the UHB IT Help Desk before any access is attempted

- Ensure that PCs and laptops which are used for homeworking are regularly brought in and connected to the network in order to receive the latest anti-virus updates at least on a monthly basis.

All staff must not:

- Load any software onto their PCs or laptops. If up-to-date or replacement software is required, a member of the IM&T Department staff must install it. This enables the IM&T Department to monitor that all software is supported by a valid supplier's licence

- Install unlicensed software on UHB equipment. If access to additional software is required requests must be made by Line Managers for this.

- under any circumstances load games software or any other unauthorised software on to a UHB PC or laptop

- Don't run or save attachments to emails from senders who are unknown to you. A favourite device used by virus writers to infect computers is to supply the virus as an attachment and persuade the recipient to execute the attached virus program.

- Don't click on any link in an email from a user or organisation unfamiliar to you.

- Don't give your email address to any website without being absolutely sure that the website is run by reputable people who will not misuse the information to add your address to spam mailing lists. Be wary about joining any mailing list not hosted by reputable organisations or by people with whom you are familiar.

- Don't ever send a reply to spam email, whether abusive or not. By replying you are confirming the existence of your email address and inviting an even greater volume of spam in future.

If unauthorised and/or unlicensed software is found on your PC or laptop this will lead to investigation and possible disciplinary procedures may be initiated.

The UHB's is responsible for ensuring:

- Anti-Virus software is installed on all computers and laptops that attach to the UHB network

- Anti-Virus files are kept up to date via the network when PCs and laptops are started up

- Email monitoring software is active and this scans all incoming e-mails to reduce risks of viruses being passed undetected. Any e-mail that appears to contain potentially harmful attachments are either quarantined or rejected.

- Users are kept informed of potential and actual malicious activity directed at the UHB network and systems

- Anti-Virus awareness is part of the induction process

- A copy of the Anti-Virus Guidance is available to all staff on the UHB intranet

3 Viruses Explained

What Is a Virus

A computer virus is a piece of software that can be transferred between programs or between computers without the knowledge of the user. They are usually designed to cause as much damage to your files as possible, rendering your data and/or PC unusable and therefore always constituting a breach of security.

How are Viruses created/How do they happen

The majority of PC viruses are written by criminals, 'hobbyists' or disgruntled employees who have one aim in mind: to develop the most undetectable, damaging viruses and to circulate them to as many users as possible.

It is often the challenge and excitement of writing a virus that will go undetected by the latest virus-checking software.

There are many virus types in circulation and only the producer of the virus will know what it was really designed to do.

The virus writer will incorporate instructions to the virus on when it should be activated and what actions to perform.

Some are made just for fun and, for example, may just produce a comical message on a certain day of the year.

Other viruses propagate themselves as quickly and as widely as possible deleting files and/or infecting programs making outbreaks difficult to contain.

Viruses can be hidden and can remain dormant until, for example, you have turned your PC or laptop on for the 100th time since having been 'infected' with the virus, and then it will go to work and lock you out from your PC whilst deleting everything from your hard disk.

Any strange messages, extra icons, abnormal disk activity, missing files, or a sudden lack of disk-space should be reported as soon as possible to the IT Help Desk.

4 How Can we Protect Against Infection

To reduce the risk of infection :

1. Virus check all media (CDs/DVDs, Memory Sticks, Portable Drives etc) before opening any files contained on the media. A virus scan on portable media can be initiated as follows :

    i. insert media
    ii. select ‘My Computer’ or ‘Computer’ icon on your desktop
    iii. right click on the device to virus check
    iv. select ‘scan for threats’ option

2. Do not open any files attached to an email from an unknown, suspicious or untrustworthy source. Viruses cannot be transferred by ordinary text files such as an email message, but can be transferred within electronic attachments sent with an email message

3. Do not open any files attached to an email if the subject line is questionable or unexpected.

4. Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered SPAM, which is unsolicited, intrusive mail that clogs up the network. UHB policy does not permit the forwarding of non-work related chain emails.

5. It is not the norm for the users to download files from the internet; and if this is the case must always ensure caution when doing so and only from reputable sites. If you're uncertain, don't download the file and contact the UHB IT Help Desk for guidance.

6. Under no circumstances should you connect a modem to your PC without first consulting the IM&T Department.

7. Check that your anti-virus software is regularly updated. The IM&T Department will ensure that all networked PCs and laptops will have an approved virus checker loaded on set up and will regularly update as and when new versions are released. New viruses are constantly

emerging; over 500 viruses are discovered each month. It is the user's responsibility to ensure that their computer has up-to-date virus checking software.

8. When in doubt, always err on the side of caution, if you are in doubt about any potential virus related situation you find yourself in, contact the IT Help Desk.

5 What to do if a Virus is Suspected or Detected

Actions to be taken by Staff

If you suspect that you may have a virus, or your anti-virus software has detected a virus, you must do the following:

1. **Immediately** - First action you **MUST** take is to power down and switch off your PC or laptop, and if you are connected to the UHB's network, **immediately** disconnect your network cable (yellow cable) from the port at the back of your PC or laptop.

2. Once first action taken you **MUST** then report any detection of a virus to the IM&T Department Help Desk immediately (West 74-5073 or East 72-5218). No further action should be taken on the PC or laptop before the IM&T Department has disinfected and ensured that the PC or laptop is virus free.

3. Final action to be taken, you **MUST** complete an e-Datix incident report.

All virus infections are IM&T security incidents and users **must** report the virus incident as soon as a virus infection has been confirmed to the IM&T Security Office via email CV.IMT.SECURITY@WALES.NHS.UK

IM&T Department Actions

The IM&T department will ensure that all required actions are taken to correct the situation following the IM&T Standard Operating Procedure (SoP) and will return the PC/laptop to the user once all issues have been rectified enabling the PC/laptop to be used once again.

If the PC/laptop is beyond repair a replacement will be provided.

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