Reference Number: UHB 429 **Version Number:** 1.1	**Date of Next Review:** 20th Sep 2019 **Previous Trust/LHB Reference Number:** Trust 133

INFORMATION TECHNOLOGY SECURITY SOFTWARE LICENSING PROCEDURE

Introduction and Aim

This document is written in support of the Information Technology (IT) Security Policy. 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 IT Security procedure of the UHB is 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 Electronic Incident Reporting Guide
Approved by	Information Governance Sub Committee
Accountable Executive or Clinical Board Director	Executive Director of Therapies and Health Science
Author(s)	Richard Williams (IT Security) Ann Morgan (Information Governance)

CARING FOR PEOPLE
KEEPING PEOPLE WELL

GIG CYMRU
NHS WALES

Bwrdd Iechyd Prifysgol
Caerdydd a'r Fro
Cardiff and Vale
University Health Board

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
01.00 ISOSP08		04/2008	Original Document
1	20/09/16	28/08/18	Review and updated to new guidance document in line with the Schedule of Revision approved by IGSC.
1.1	20/09/16	28/08/18	Admin changes to reflect current contact details

Contents Page

1	INTRODUCTION	4
2	RESPONSIBILITIES	5
3	CONTROL OF PROPRIETARY SOFTWARE COPYING	6
4.	BENEFITS OF UHB SOFTWARE LICENCING CONTROL	6
5	COMMUNICTION	7

Appendix 1 – Useful Contacts

1 INTRODUCTION

1.1. Purpose of the Software Licensing Procedure

This document is required as the UHB needs to ensure it prevents the use of software that is either illegal or unauthorised which would constitute a very real risk to the UHB.

There are many forms of illegal software and caution must be exercised when buying software. Unauthorised software, ‘Freeware/Shareware’ downloaded from the Internet or other digital media, **must not be installed on the UHB equipment under any circumstances** as the use of such software increases the risk of introducing computer viruses and breaches the UHB’s IT Security Policy which is a disciplinary offence).

All software purchases must be authorised by IM&T via the UHB Procurement Department.

1.2. The Need for Software Licensing and Procedures

Data stored in the UHB information systems represent an extremely valuable asset. The increasing reliance of the UHB on information technology systems for the delivery of health care makes it necessary to ensure that the system software is developed, operated, used, maintained and legally licensed.

The design and development of software creates intellectual property which the law recognises through copyrighting and is covered by the Copyright, Designs and Patents Act 1988. Law. Copyright Law. In summary the following applies:

- computer software is defined as a literary work.
- infringement of copyright is not just a civil issue.
- you do not have to sell copied software to breach the law.
- the chief executive, board members and individual staff members can be personally charged and risk unlimited fines and two years imprisonment.

There are no mitigating circumstances and the UHB will not condone or defend either illegal copying or the use of unauthorised software.

This procedure sets out how the UHB will address these requirements in operational terms.

1.3 Scope of the Procedure

Good software management brings improved IT security and control to the UHB:

- maintain a software health check by controlling the procedure for buying, installing, maintaining and disposing of software.

- assist with audit of both hardware and software in establish a full picture of what the UHB currently has.

2 RESPONSIBILITIES

All Staff
This procedure applies to all UHB staff who access the UHB IT network and applies to both on and off site access using devices provided by the UHB. It is the responsibility of all staff to reduce to a minimum the dangers of introducing malicious software into UHB systems.

If any employee is unsure about any aspect of this procedure and its application to them, they should seek advice from their line manager as failure to comply with this procedure will be viewed as a serious matter and may result in disciplinary action

Department Heads must ensure

- Only authorised licensed software is installed on PCs under their control
- Any other licensed software, not procured directly by the UHB, such as that used for training purposes, or software as an element of authorised licensed software is compliant with all software licensing conditions. For equipment linked into a central system, permission will also be needed from the Head of IT.
- Contracts for software development to be written specifically for the UHB must be in consultation with the IM&T Department and that suitable arrangements are made for the copyright to be vested in the UHB. Copyright will be vested in the UHB for all software written by staff in the course of their employment.
- They register all software with the IM&T Department. Possession of media is not proof of ownership and further investigation may be necessary.

Managers must ensure

- They contact IT Services (Development Manager) for confirmation of acceptability of proposed new system requirement on the UHB IT network
  - Once IT Development Manager and IT Security Manager approved, all software orders are to be processed through the UHB Procurement Department
- They advise IT Helpdesk of requirement for installation of all new software onto the UHB network
- They indicate official Software License information to IT Helpdesk at time of installation, in order for network asset registration
- They retain a register of Software License and any renewal dates and costs applicable within their area.

Managers must not

- Directly procure and/or install software applications without following this procedure

All Staff must ensure

- They only use system applications they have access to, and in an appropriate manner at all times
- They retain the strict confidentiality of all/any information to which they have access

All Staff must not

- Load software packages onto UHB provided PCs, laptops, networked devices or UHB network servers without authorisation from IM&T IT Security.
- **On any account** load 'games software' on staff UHB provided PCs or laptops.

3 CONTROL OF PROPRIETARY SOFTWARE COPYING

Legislative and contractual requirements place restrictions on the copying of software. In particular, they may require that only software that is developed by the UHB or that is licensed or provided by a third party to the UHB can be used.

Proprietary software products are usually supplied under a licence agreement, which limits the use of the products to specified machines, and may limit copying to the creation of back-up copies only.

It is the UHB's policy to comply with all legal obligations, and to ensure that no copyright material is copied without the owner's consent.

Users must not contravene the policy by copying software from one machine to another without the owner's documented authority.

Copying of proprietary or UHB software, for use on computers which do not belong to the UHB, for any purpose other than that which is fully authorised UHB business, might similarly infringe copyright, and will be in breach of UHB policy.

Where it is necessary to use a software product on additional machines, additional licence copies or copies are to be purchased.

Copyright infringement can lead to legal action, and perhaps criminal proceedings, against the UHB and the individual concerned.

4 BENEFITS OF UHB SOFTWARE LICENCING CONTROL

Better use of existing software investment, by identifying how many and what types of licence is held and then moving unused software licences to the departments where they are needed, rather than buying new copies.

Increased productivity due to the most appropriate software being used for the task in hand.

A reduction in software expenditure as a policy of standardising on selected packages will improve purchase power on new and upgraded software.

Data security will improve by avoiding the risk of virus being transmitted by uncontrolled copying.

Prevent the uncontrolled introduction of unauthorised software (e.g. games software) that leaves the UHB exposed to virus infections that can spread rapidly through networks and on digital media through the transmission of data between systems

5 COMMUNICATION

- this procedure should be brought to the attention of all staff

- copies of this procedure is available to all staff and can be obtained from; the UHB's intranet site, IT Security Manager or email CV.IMT.SECURITY@WALES.NHS.UK

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