GIG CYMRU NHS WALES Bwrdd Iechyd Prifysgol Caerdydd a'r Fro Cardiff and Vale University Health Board	**Reference Number: UHB 254** **Version Number: 1** **Next Review Date:31/03/18** **Previous Trust/LHB Reference Number: N/A**

INFORMATION TECHNOLOGY SECURITY POLICY

Policy Statement

Cardiff and Vale University Health Board (the UHB) relies on information technology (IT) systems to record, manage and inform its clinical and business processes. The data stored in the UHB's information systems represents an extremely valuable asset. Furthermore the UHB has a statutory obligation to ensure the safe processing i.e keeping, secure use, handling, maintenance and storage of information and data held within its information technology systems.

The UHB will make sure that it processes information safely and securely in accordance with legal requirements, codes of practice and guidance issued by relevant authorities including but not restricted to the Information Commissioners Office.

The mechanism of control for this is referred to as Information Governance within which Information and IT Security (ITS) sits. The Information within this scope may be personal (relating patients and employees) and corporate (for example financial records, letters, reports etc) and in virtual or physical format.

The legislation and guidance that the UHB has to follow are shown below:

Legislation

- The Data Protection Act 1998.
- The Computer Misuse Act 1990
- The Health and Safety at Work Act 1974
- The Freedom of Information Act 2000
- The common law duty of confidentiality.
- Environmental Information Regulations 2004
- The Human Rights Act article 8. 1998
- The Mental Health Act 1983
- The Health and Social Care Act 2001

Information security is governed by UK legislation and EU directives. See the list of legislative acts above. Please note that this list is not exhaustive:

Other guidance and UHB policies that are complementary to this policy are:

- Caldicott Principles
- NHS Confidentiality Code of Practice

Supporting procedures and other written control documents translate these principles into more detailed instructions or guidance including individual responsibilities.

Policy Commitment

The UHB aims to establish and maintain the security and confidentiality of information, information systems, applications and networks used by the UHB.

The UHB has set five key objectives in order to achieve the aims of this Policy by safeguarding the key elements of IM&T data security. The UHB will safeguard:

- **Confidentiality** - by ensuring that access to information and data is confined to those people with specific authority and rights to do so.
- **Integrity -** by ensuring that information and data is entered accurately, in a timely manner and is complete.
- **Accessibility** – by ensuring that all the UHB's systems, assets and networks are operational and are maintained .
- **Availability** – by ensuring that that information is available and delivered to the right person at the time it is needed.
- **Network security** – by ensuring that the infrastructure of the UHB complies with legal, national and local requirements.

The UHB shall put arrangements in place to establish and maintain the security and confidentiality of information, information systems, applications and networks used by the UHB.

These arrangements shall include a corporate training programme designed to meet staff needs at all levels in line with their level of responsibility.

All employees are required to adhere to this policy. Inappropriately accessing or using information may lead to disciplinary action. Serious breaches, for example inappropriate disclosure of person identifiable information, theft and misuse of information technology may constitute gross misconduct, lead to dismissal and may possibly require police involvement.

Supporting Policies, Procedures and other Written Control Documents

This policy and the supporting guidance together with its procedures describe the UHB's aims, objectives and operational organisation in regard to discharging its obligations in respect of Information and Technology Security.

Scope

This policy applies to all UHB staff whether permanent, temporary, or contracted (including students, contractors or volunteers in all locations including those with Honorary Contracts.

Equality Impact Assessment	An Equality Impact Assessment has been completed for the overarching IG Policy. 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 Policy	Information Governance Policy Risk Management Policy Risk Assessment and Risk Register Procedure UHB Corporate Risk and assurance Framework Guide to Incident Reporting Incident Management Investigation and Reporting. [Serious incidents] Access controls IM&T Security Breaches Business Continuity Management Security of Assets Off-site Mobile Computing Policy Remote Access Software Protocol
Approved by	People, Performance and Delivery Committee
Group with authority to approve procedures written to explain how this policy will be implemented	All policies will be approved by the People, Performance and Delivery Committee All supporting procedures will be approved by the Information Governance Sub Committee
Accountable Executive or Clinical Board Director	Executive Director with responsibility for Information Technology
Author(s)	Head of Information Governance and Assurance

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the mos 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	31 Mar 2015	10 Apr 2015	New policy