INFORMATION ASSET POLICY

Executive Sponsor & Function:

Board Secretary

Document Author:

Deputy Director Planning, Performance & Digital

Approved by:

Executive Team

Approval Date:

22 May 2019

Date of Equality Impact Assessment:

14/03/2019

Equality Impact Assessment Outcome:

This policy has been screened for relevance to equality. No potential negative impact has been identified so a full equality impact assessment is not required.

Review Date:

May 2022

Version: v1

EXECUTIVE SUMMARY
INFORMATION ASSET POLICY

Overview:	Health Education and Improvement Wales (HEIW) has access to a wide range of highly sensitive information in relation to its functions. This policy provides details on the expectations and responsibilities of staff in relation to the management of such information.
Who is the policy intended for:	Everyone working for or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts.
Key Messages included within the policy:	The key objectives of the policy is to: • advise staff of their responsibilities in relation to managing information assets in the course of operational functions and the key responsible individual key to the success of this policy.

PLEASE NOTE THIS IS ONLY A SUMMARY OF THE POLICY AND SHOULD BE READ IN CONJUNCTION WITH THE FULL POLICY DOCUMENT

Contents Page

1. Policy Statement

It is the policy of HEIW that all manual and electronic records containing personal data are identified, categorised, classified, recorded, and managed. In order to achieve this, an Information Asset Register must be used to catalogue all of the organisations information assets.

2. Purpose

The Policy also sets out the responsibilities of any staff/trainees responsible for activities covered by this policy.

These responsibilities include, but are not restricted to, ensuring that:

- The availability of information assets are known, clear, concise and maintained in line with current business responsibilities;
- All individuals as referenced within the scope of this policy are aware of their obligations;

This policy must be read in conjunction with relevant organisational procedures.

3. Scope of this Policy

This policy applies to everyone working in or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts with a responsibility connected with this policy.

This policy applies to all manual and electronic records containing personal data regardless of the location where it is stored.

4. Aims of the Information Asset Policy

4.1 Identification of Information Assets

An ‘information asset’ for the purpose of this policy, will be any asset, held manually and/or electronically, which contains information relating to any person whether living or dead.

4.2 Asset Management

Each information asset must have an assigned Information Asset Owner. The Information Asset Owner will be responsible for implementing and managing controls to protect the integrity of that information.

Responsibility for implementing and managing these controls may be delegated, however accountability must remain with the nominated Information Asset Owner.

The Information Asset Owner must know:

- the information that is held and the nature of that information
- details of those who has access and the purpose for their access

Information Asset Owner shall provide reports to the Senior Information Risk Owner (SIRO) and the Data Protection Officer at least annually to provide assurance on the use of the information asset.

4.3 Categorisation of Information

Information assets which relate to a person, whether living or deceased, must be recorded in a register. A register must hold details of the systems on which the information asset is held.

Information asset shall be categorised as personal data or special categories of personal data. For the purpose of this policy, special categories of personal data will refer to any information that consists of a person's health or sexual orientation information, religion, race or ethnic origin, political opinion, trade union membership, genetic, and biometric data where processed to uniquely identify an individual.

4.4 Data Quality

Local data quality audits must be undertaken and documented by the Information Asset Owner on a regular basis. Local data quality issue logs must be implemented and maintained.

4.5 Information Risk Management

An Information Asset Owner should undertake a risk assessment for any information assets that they own. The Information Asset Owner must ensure that information risk assessments are performed at least once a quarter. Controls on information must remain in place throughout the lifetime of an Information Asset.

4.6 Business Continuity

Information Asset Owners must have approved Business Continuity Plans in place. This will form part of the wider organisational Business Continuity Plan. Procedures should be in place to detail the specific actions which should be undertaken if the Business Continuity Plan was to be invoked. All staff/trainees who access systems which contain an information asset must be notified of business continuity arrangements and receive any training and guidance as may be necessary to implement these arrangements. Business Continuity plans and the associated procedures which relate to asset management must be regularly tested.

4.7 Asset Disposal

Information assets must be retained in line with NHS Wales Policy and guidance. Data must be made available for operational and client use for as long as is necessary to

perform the required business function. Any instructions to destroy information must be signed off by the responsible Senior Information Risk Owner, Data Protection Officer or in the case of clinical information, the Caldicott Guardian. Where this occurs, details of the deletion must be held on a register detailing the date, time, method and personnel responsible.

4.8 Requests for information

HEIW is keen to ensure that all information it holds is made available where this is a legal requirement to do so.

Information Asset Owners must cooperate in providing information to the designated lead where a request for any information has been received. Designated leads within the organisation must at all times ensure that any disclosure is lawful and protects the confidentiality of the person who the information is about.

4.9 Training and Awareness.

Everyone working for or engaged by Health HEIW including part time workers, temporary and agency workers and those holding honorary contracts who need support in understanding the legal, professional and ethical obligations that apply to them should contact the Information Governance Manager.

5. Responsibilities

The policy applies to everyone working for or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts. Everyone working for or with the NHS who records, handles, stores, or otherwise comes across information has a personal common law duty of confidence to individuals referred to in that information.

5.1 Chief Executive

The Chief Executive is responsible for ensuring the highest level of organisational commitment to the policy and the availability of resources to support its implementation and any associated legal requirements. Responsibilities may be delegated to HEIW and Senior Information Risk Owners, Data Protection Officers and/or Caldicott Guardians as appropriate.

5.2 Senior Information Risk Officer

The Senior Information Risk Officer (SIRO) is responsible for taking ownership of the organisation’s information risk policy and for acting as an advocate for information risk. The Senior Information Risk Officer are also responsible for monitoring the process by which all information assets are identified and reviewed.

In HEIW the SIRO is the Board Secretary.

5.3 Caldicott Guardian

The HEIW Caldicott Guardian is the Medical Director and he/she is responsible for protecting the confidentiality of health and care information held by their respective organisation and for enabling appropriate information sharing by ensuring that information is used properly. Together with the respective Senior Information Risk Officer, they are responsible for monitoring the process by which all information assets information are identified and reviewed.

5.4 Managers

Managers are responsible for the implementation of this policy within their department. In addition, they must ensure that their staff/trainees are aware of this policy understand their responsibilities in complying with the policy requirements and are up to date with mandatory information governance training. Breaches of the policy must be reported via local incident reporting processes and dealt with in line with the relevant Workforce and OD policy where appropriate.

5.6 Staff

Staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area as appropriate. Mandatory Information governance training must be undertaken at least every two years. Breaches of this policy must be reported via local incident reporting processes.

6. Available Guidance

Guidance on the procedures necessary to comply with this Policy should be made available by HEIW on its web pages. Managers will be responsible for ensuring that all their staff are made aware of HEIW policies and standards.

7. Monitoring

HEIW notifies details of the personal data it processes to the Information Commissioner for inclusion on the register of Data Controllers. The notification is reviewed annually by HEIW. The register is maintained by the ICO and is available in the public domain for inspection by anyone

The policy will be reviewed every 3 years, unless where it will be affected by major internal or external changes such as:

- Changes in Legislation;
- Practice change or change in system/technology; or
- Changing methodology.

8. Equality

In accordance with HEIW's Equality policy, this Policy will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin,

sexual orientation, marital status, religion or belief, age, union membership, disability, carer's status, offending background or any other personal characteristic.

9. Contacts

For further advice and/or assistance on how to ensure individual and associated organisational compliance with this Policy, please contact local Information Governance department.

10. Further Information

This Policy should be read in conjunction with the following HEIW policies:

- Data Protection & Confidentiality Policy
- Information Governance Policy
- Confidentiality Breach Reporting Policy
- Records Management Policy
- Freedom of Information Act Policy
- Data Quality Policy
- Information Security Policy
- Email Policy
- Internet Use Policy
- Social Media Policy