INFORMATION SECURITY POLICY

Executive Sponsor & Function:

Board Secretary

Document Author:

Deputy Director of Planning, Performance and Digital

Approved by:

HEIW Executive Team

Approval Date:

29 January 2020

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:

January 2023

Version: v1

Contents Page

Overview:	To ensure that where any need exists to make use of, process and/or share any information that this is carried out in an appropriate manner and only between those who need to use the information; whilst also protecting information from any unauthorised access and loss. For the purposes of this policy that: - • All systems are properly assessed for security; • Confidentiality, integrity, availability and suitability of information are maintained; • Staff are aware of their responsibilities; • Procedures to detect and resolve security breaches are in place.
Who is the policy intended for:	All persons employed or engaged by Health Education and Improvement Wales (HEIW) including part time workers, temporary and agency workers and those holding honorary contracts.
Key Messages included within the policy:	• Staff are aware of the basic principles of information security • Key responsibilities highlighted • Highlighted active information security advice when managing sensitive information and procedures to follow
PLEASE NOTE THIS IS ONLY A SUMMARY OF THE POLICY AND SHOULD BE READ IN CONJUNCTION WITH THE FULL POLICY DOCUMENT	

1. Policy Statement

The Health Education and Improvement Wales (HEIW) Information Security Policy sets out and affirms HEIW's commitment to continued compliance with applicable legislation, directives and standards regarding the security and governance of information.

HEIW holds and uses a great deal of information, much of it personal and confidential, and without which the HEIW could not function. The HEIW places a very high importance on the security of any information that it maintains and recognises the role of information security in ensuring that its staff/trainees and others have access to information that they require.

2. Purpose

The purpose of this policy is to ensure that where any need exists to make use of, process and/or share any information that this is carried out in an appropriate manner and only between those who need to use the information; whilst also protecting information from any unauthorised access and loss.

For the purposes of this policy that: -

- All systems are properly assessed for security;
- Confidentiality, integrity, availability and suitability of information are maintained;
- Staff are aware of their responsibilities;
- Procedures to detect and resolve security breaches are in place.

3. Scope of the Policy

This policy applies to HEIW's arrangements for creating, collecting, storing, safeguarding, disseminating, sharing, using and disposing of information in accordance with applicable legislative responsibilities, stated objectives and relevant standards.

The Policy applies to all persons employed or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts. regardless of the location at which access to the information is gained.

It applies to all forms of information processed by HEIW and covers all business functions and the information, information systems, networks, physical environment and relevant people who support those business functions. This includes paper records, spoken word, computer records, magnetic media, imaging systems, and to the collection and dissemination systems and processes of the information such as transmitted across networks, mail, facsimile or telephone.

4. Aims of the Information Security Policy

The aim of this policy is to ensure that all staff are aware of and comply with relevant legislation requirements and security standards whilst ensuring information is held safe and used appropriately to assist in the delivery of service by promoting good practice, preventing and minimising the impact of information security incidents.

4.1 Key Principles of the Policy

The basic principles of information security that will be applied to all information and information systems are those of confidentiality, integrity, accessibility and suitability:

- **Confidentiality:** HEIW stores information from a range of sources. HEIW has a legal responsibility, which is shared by its all persons employed or engaged by HEIW to ensure that this data is not accessible to anyone without appropriate authorisation.

- **Integrity:** HEIW has a duty to ensure that the data it holds is accurate, and remains so throughout the time it is held. It safeguards the accuracy and completeness of information through the use of approved processes to ensure that precautions are taken to ensure that the data is not changed through accidental misuse, deliberate abuse or even through the failure of a computer system to store it properly.

- **Accessibility:** HEIW must ensure that the people who depend on particular items of information gain timely access, whilst ensuring that the information is only available to authorised people when needed.

- **Suitability:** HEIW must ensure that all systems are suitable for the desired task, and where appropriate, are compliant with the recommendations of regulatory bodies.

Any reduction in the confidentiality, integrity or availability of information could prevent HEIW from functioning effectively. Moreover, the unavailability or loss or unauthorised disclosure of information has the potential to harm individuals (e.g. staff/trainees), damage the HEIW's reputation and cause financial loss.

5. Legislation/Standards

The need for information security and for the HEIW to re-consider current practices has arisen from statutory provisions and good practice guidance documents that include but are not limited to:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- The Computer Misuse Act 1990
- Electronics Communication Act 2000
- The Regulation of Investigatory Powers Act 2000
- Caldicott Report 1997
- ISO27001 Information Security Standard

6. Responsibilities

HEIW recognises its corporate responsibility and commitment to compliance with Information Security requirements; as stated within statutory provision and good practice guidance, and to further raise staff/trainees awareness of good Information Security practices. Responsibilities that include ensuring: -

- All information users are provided with appropriate information security training;
- Compliance with this policy and related policies, local procedures and instructions, and ensure that any changes are also communicated;
- Users only have access to information that is appropriate to their role within the organisation;
- Reported incidents are properly investigated and resolved;
- Assess risks to information security and act to reduce those risks;
- All staff should comply with the information security policy.
- Terms and conditions contained within employment contracts include an undertaking to maintain confidentiality of information at all times and will continue to apply even after the contract of employment has ended.

6.1 Chief Executive

The Chief Executive takes overall responsibility for information security

6.2 NHS Wales Informatics Service

NHS Wales Informatics Service (NWIS) is responsible for:

- Managing the technical security controls within the IT infrastructure and information systems.
- Provisioning, securing and change control of business systems including networks, internet services, SharePoint and Office 365.
- Provisioning and secure the network infrastructure, managing the anti-virus software.
- User account management, password policy and access controls on SharePoint, Outlook, laptops and access to network resources.
- Technical security controls that meet the agreed international (ISO) and British (BS) standards;

6.3 Board Secretary

The Board Secretary is responsible for:

- An independent reporting line to the Chief Executive for suspected information security incidents involving normal management lines;
- The production of business cases for the procurement or development of information systems includes compliance with relevant policies and include technical security controls;
- Ensuring the identification of ‘systems managers’ for all information systems;
- Technical security controls that meet the agreed international (ISO) and British (BS) standards;

6.4 Directorate Directors

Directorate Directors are responsible for:

- Ensuring that their department complies with this policy;
- Conduct regular audits to monitor compliance with this policy;
- Ensuring all persons employed or engaged by HEIW are aware of the requirements incumbent upon them;
- Delegating the day-to-day responsibility to information security leads and information security and governance groups as defined by the Divisions and as appropriate to their needs.

6.5 Caldicott Guardian / Medical Director

The HEIW has a Caldicott Guardian. It is the Medical Director and as such:

- Have delegated responsibility to ensure compliance with the confidentiality, security legislation and guidelines of the Caldicott Report;
- Have the authority to approve protocols and policies if the Information Governance and IM&T Committee cannot meet;
- Appoint a delegate who will have the same authority when the Caldicott Guardian is unavailable.

6.6 Employee Responsibilities

Every person employed or engaged by HEIW is responsible for their own actions and must:

- Comply with this policy with its corresponding policies, protocols and procedures;
- Apply the basic principles of information security to all information, which they come into contact with;
- Discuss any identified risks and security issues with line management;
- All persons employed or engaged by HEIW are personally responsible for ensuring that no actual or potential security breach occur as a result of their actions;
- Report incidents as soon as possible by following HEIW's incident reporting procedure;
- Operate a clear desk and clear screen policy. This means that personally identifiable or organisationally sensitive information must be placed out of sight, in locked cabinets when not in use, and it should not be viewable on screen by anyone who does not have a legitimate need to see it.
- All persons employed or engaged by HEIW.who have been supplied with portable equipment (i.e. laptops or similar devices) are responsible for ensuring that it is regularly connected to the HEIW network to ensure that upgrades for anti-virus software are installed.
- Casual staff/trainees and third parties not covered by an employment contract will be required to sign a confidentiality agreement before being given access to information processing facilities.

6.7 Information Governance and IM&T Group

The IG and IM&T group is responsible for:

- Authorising the Information Security Management System;
- Authorising HEIW information security policies and protocols;
- Authorising HEIW information sharing policies and protocols;
- Monitoring compliance with the IG and IM&T policies

7. Active Information Security

7.1 Controlling Access

Access to computer services and to data will be controlled on the basis of business requirements, which take account of policies for information, dissemination and entitlement.

System Managers will ensure that appropriate security controls and data validation processes, including audit trails, will be designed into application systems that store any information, especially personal data.

7.1.1 Staff/trainees

Access to all HEIW systems are controlled by user names and passwords. All new staff/trainees wishing to apply for a user name, all staff/trainees wishing to change their current access levels and all notifications of staff/trainees leaving must follow the relevant instructions for the system.

7.1.2 3rd Party Access

All 3rd party access can be achieved via N3 or Secure ID Token with the relevant Statement of Compliance approval.

7.2 Computer Security

To ensure the confidentiality and security of the data held electronically the following controls must be complied with at all times:

- All PCs and Laptops will have a standard operating system and managed desktop environment.
- All PCs and removable media used to process personally identifiable or organisationally sensitive information must be encrypted unless otherwise risk assessed (i.e. Medical Devices). Contact the IT Service Desk for further details.
- Always log off or lock your computer (using Ctrl, Alt & Delete or Windows key & L) before leaving it unattended.
- Do not allow unauthorised persons access to your computer.
- Do not try to connect unauthorised devices to HEIW's network e.g. modems, CD drives, iPods etc
- Do not move your desktop computer without first contacting the IT Service Desk. Where appropriate computers should be secured (via a steel cable to an anchor point) and security marked. Contact the Service Desk for further details.
- Do not tamper with computer equipment or remove any components as this may invalidate the warranty, may endanger your safety and may be deemed as theft. All component changes are tracked using HEIW's asset management software.
- All computer equipment must be security marked and locked with a suitable security device. This does not apply to portable computer equipment.

- Use of HEIW computers by anyone other than the authorised employee is strictly prohibited.
- 3rd Party Cloud storage (i.e. dropbox) must not be used to store business or staff related information.
- Removable media (i.e. laptops, USB sticks, etc) must not be left in cars, even if secured out of view, or left unattended in public areas, this includes but not limited to: -
    - public transport
    - food & drink outlets

7.3 Correct use of Passwords

- Do not try to log onto systems that you are not authorised to use.
- Comply with the national guidance on secure passwords.
- Do not log in using another person's user name and password.
- Do not share your password.
- Do not write your password down.
- Where a user has forgotten his/her password and are unable to reset their Password using the system provided, they should contact either the relevant System Manager for clinical systems or the IT Service Desk where assistance will be given.
- Do not store passwords in any program macro or function key.

7.4 Removable Media

Removable Media devices include: USB Flash Drives, MP3 players, mobile phones/camera phones, cameras and Personal Digital Assistants (PDAs) such as Palm Pilot, iPAD devices. Portable storage media also includes CDs, floppy disks, tapes, etc.

- All persons employed or engaged by HEIW may not attach any personal removable media devices other than USB Memory Sticks to the HEIW network without prior permission of the IT Department.
- Encrypted Removable Media must be used whenever Users need to process personally identifiable or organisationally sensitive information away from the HEIW and then only if it is absolutely essential and in connection with their duties.
- All unencrypted USB sticks will be rendered "Read only" by security software.
- Removable media must not be left unattended except within secure official buildings.
- Removable media must not be left in cars, even if secured out of view, or left unattended in public areas, e.g. public transport, food & drink outlets.
- The user must be responsible for ensuring that no unauthorised person has access to the data held on the removable media both during and outside normal working hours - this includes access by family members if the removable media is used within the home.
- It is not permissible to copy any personally identifiable information to personal computers in the home.
- Removable media such as memory sticks, floppy disks, CDROMs etc must be disposed of by contacting the IT Service Desk who will advise you on the correct procedures to be followed.

7.5 Disposal of Computer Equipment

The following will apply to computers and other IT equipment identified as redundant or obsolete:

- Any IT equipment identified as being redundant or obsolete by either the IT Department or the Department Manager can be collected at a mutually convenient time.
- Whenever possible, the IT Department will endeavour to reuse reconfigured and sanitised equipment for use elsewhere within the organisation. Where this is not feasible the equipment will be securely disposed of in accordance with IT Department operational procedures.
- HEIW's IT asset register will be updated to reflect the status of the newly disposed equipment.

7.5.1 Disposal of Removable Media

For the purpose of this policy 'removable media' can be defined as any device that can be used to store electronic copies of data and which provides a removable, mobile medium for the transportation of this data. This includes but is not limited to the following:

- CD and DVD,
- 3.5" floppy diskettes,
- high-density tapes,
- USB memory sticks,
- flash memory cards,
- Corporate mobile phones
- Personal Digital Assistants

Delivery must be in person and a receipt must be obtained from the IT Department.

Use of the mail service is not appropriate for transporting removable media.

Removable media must be disposed of by contacting the IT Service Desk who will advise you on the correct procedures to be followed.

Where the recycling of the removable media is an option, the IT Department will thoroughly erase any data that might reside on the media prior to reuse.

7.6 Security Audits

HEIW reserves the right to monitor use of any access to the HEIW's network. This encompasses all applications, network access and includes Internet access and email usage.

Reasons for monitoring include:

- Ensuring that the HEIW's policies and procedures are adhered to.
- Preventing or detecting unauthorised use or criminal activities.
- Maintaining the effective operation of the HEIW's communication systems.

Compliance with this policy will be monitored via a programme of security audits. Ad hoc audits may be undertaken by the IT Department at the request of Directors, Departmental Heads and/or other Senior Management.

7.7. Physical Security

Appropriate measures must be taken to protect all IM&T equipment against loss or damage and to avoid interruption to business activity.

Do ensure that local physical security procedures are followed. Security doors must be closed, properly locked and entry codes changed regularly.

Disposal of any organisational IT equipment and/or media must be carried out by a member of the IT Department, and with the knowledge of the relevant Systems Data Owner.

7.8 Controls against malicious software, malicious actions and viruses

HEIW will seek to minimise the risks to software and information from viruses through education, good practice / procedures and by ensuring that the most up to date anti-virus software is utilised on all PCs, Laptops and Servers. The unauthorised configuration of anti-virus settings by anyone other than HEIW IM&T staff is prohibited. Any detected or suspected computer viruses must be immediately reported to the HEIW IT Department.

All software installed must be appropriately licensed. The use of unauthorised software is prohibited. The maintenance of a register of software assets and licence compliance will be managed by the IT Department.

Users who have been supplied with portable equipment (i.e. laptops or similar devices) are responsible for ensuring that it is regularly connected to the HEIW network to ensure that upgrades for anti-virus software are installed.

7.9 Storage and Copyright Law

Only authorised freeware or shareware can be installed on HEIW computers. Do not install unauthorised or unlicensed software. Software can only be installed by members of staff/trainees authorised to do so. It is a criminal offence to use illegal copies of software programs for which both the HEIW's Directors and individual employees may be liable if this policy is not complied with. Any employee illegally and knowingly reproducing software will be subject to the HEIW's disciplinary procedure.

All information and data stored on the HEIW's equipment is deemed to be HEIW property. Copying or storage of anything that is not work related onto your computer is a breach of this policy.

Do not allow anyone to take unauthorised copies of software. HEIW owned software must not be taken home and loaded / installed onto an employee's home computer. If an employee has to use software at home for HEIW business, and is not provided with a HEIW computer for this purpose, a separate copy of the software must be purchased for the home computer.

All software, information and programs developed for and / or on behalf of the HEIW by employees during the course of their employment will remain the property of the HEIW. Duplication or sale of such software without the prior consent of the HEIW will be considered an infringement of the organisation's copyright and will be dealt with as a disciplinary matter.

HEIW computer equipment must not be used for any of the following activities:

- The copying, saving or distribution of copyright media files e.g. MP3 or MPEG, games files, audio CDs or video DVDs
- The playing of games files or illegally copied audio, video or digital music files e.g. MP3 / MP4.
- No content that may be deemed as either illegal or offensive may be kept on any HEIW equipment.
- Sending, receiving or storing of private photographs is prohibited

7.10 Energy Saving

- Do log out and turn off all computer equipment (base unit and screen) at the end of the day and turn the power off at the wall socket where possible.
- Do turn off printer and photocopying equipment as above.

8. Portable computers and home working

All persons employed or engaged by HEIW are responsible for the portable computer equipment in their care and as such must ensure that it is kept secure at all times. Place portable equipment out of sight whenever possible and preferably lock it away.

Such equipment must always be properly secured, both in your office and whilst travelling. Extreme caution must be adopted if being used within public areas and never leave devices unattended. Protect remote access procedure documentation, secure-id user names and PIN numbers. Keep these items physically separate from the computer and carrying case.

Report a loss or theft of laptop and/or any portable equipment immediately to the police and relevant manager. It is the manager's responsibility to ensure that this is also reported through the HEIW's Incident Reporting Procedure.

Do not store confidential or personal identifiable information (PII) on portable computers unless it is encrypted. This information must always be securely deleted as soon as possible. **Contact the IT Department if your laptop is not encrypted.**

If you are working on sensitive information be aware of the environment and ensure the screen or documents you are working on cannot be seen by others. Working on sensitive or PII in a public area should only take place when it is absolutely necessary.

Do not install software, regardless of its licence status, on HEIW portable computers. Any requirement for software should be discussed with the IT Department who will, if appropriate, facilitate its installation.

Ensure that information or programs no longer needed are effectively erased from all equipment and media. If you are unsure of how to do this contact the IT Service Desk for advice and guidance.

Do not save PII or confidential information to portable storage devices, e.g. Memory sticks unless they are encrypted. Contact the IT Department if you require help.

HEIW equipment must not be used to access the World Wide Web on home Internet connections unless achieved by using the HEIW approved connection software.

All security and monitoring software installed on portable computer equipment must not be disabled at any time.

9. Information Governance

When dealing with all types of information please be aware of the requirements of the HEIW's Record's Management policy with regard to the retention and disposal of this information.

When transporting or transferring data outside the HEIW be aware of the data protection and confidentiality policy and always check with the Information Governance Department or the Information Security Department who can provide guidance.

The distribution and storage of person identifiable information is governed by the Data Protection Act 2018. To ensure that person identifiable information is dealt with correctly you must follow the guidance in the HEIW's Data Protection and Confidentiality Policy, or if you have any queries contact the Information Governance Officer.

Do not store confidential, person identifiable or business sensitive information on your computer's local hard disk drive. Store it on an appropriate network drive where it will be secure and backed up on a daily basis. Saving data to the network aids sharing of this information where necessary.

All persons employed or engaged by Health Education and Improvement Wales (HEIW) have a duty to ensure all confidential/person identifiable information is recorded accurately and in a timely manner. If such information is found to be inaccurate on a system, it must be corrected either at source, or with assistance from the relevant system manager and/or Department.

When exchanging person identifiable information with external agencies e.g. social services, ensure you comply with the relevant section in the Welsh Accord for the Sharing of Personal Information (WASPI). This protocol informs what information can be exchanged and what controls need to be put in place to ensure the safety of that information. Contact the Information Governance Department if you are unsure.

Do not attempt to access, or ask people to divulge information that you are not authorised to receive; e.g. Information relating to a family member or a friend. Do not divulge information to those that are not authorised to receive it.

Do not leave confidential documents unattended, particularly on printers, photocopiers, fax machines or on desks.

Do not make unauthorised copies of confidential information.

HEIW provides containers (i.e. confidential waste bins) for the secure disposal of confidential and person identifiable information, ensure these facilities are used at all

times. Do not dispose of any personally identifiable, confidential and/or organisationally sensitive information within domestic bins.

HEIW will make available, in a controlled manner, personal or information it holds in its offices required under statutory arrangements, to aid clinical and/or negligence investigations or to assist the Police if such information is required as part of a criminal investigation.

10. Internet Use

Guidance on the use of the Internet and the procedures to be followed for authorising Internet access can be found within the HEIW's Internet Access policy on the HEIW's Intranet site.

11. Email Use

Guidance on the use of the HEIW's E-mail system and the procedures to be followed for authorising E-mail access can be found within the HEIW's E-mail policy on the HEIW's Intranet site.

12. Employee Leaving Procedure

For further information on how to register employee terminations please refer to the instructions on the HEIW Intranet. All managers must ensure they follow the HEIW procedures for employee leaving and ensuring all HEIW equipment e.g. Laptop, Secure-id token, memory sticks, door entry tokens, mobile phones, etc are returned.

On receipt of a resignation, line managers must discuss with the individual which parts of their email account should be retained for business continuity purposes and share or forward any information required by the department to other staff/trainees as directed. A user's e-mail account will be hidden for 28 days after their last working day. After the 28 days the contents of the mailbox will be deleted and the account will be disabled.

Managers are required to inform the IM&T Department of employees who are expected to be absent from the HEIW for a significant period of time e.g. on maternity leave or long term sick leave as these accounts can either be disabled until the user returns to work, an appropriate 'out of office' message can be set up or delegated access can be granted to another person within the department.

13. Security Incidents

Any actual security incident should be reported using the HEIW incident reporting procedure.
If you suspect your workstation has a virus or malicious software on it, report it immediately to the IT Service Desk and the NWIS Service Desk.

In the case of unintentional or accidental access to inappropriate material (e.g. pornographic internet popup messages), inform the IT Department immediately (or as soon as possible for incidents occurring out of office hours), giving as much detail of the incident as possible. The incident can then be verified against the Internet security logs. Failure to report known incidents may result in disciplinary action.

14. Training

All new staff/trainees must attend an awareness session where appropriate information security training is given. This must be provided at the earliest opportunity and without delay.

Awareness sessions are scheduled regularly across the HEIW and will inform staff of their responsibilities in relation to confidentiality of data, Freedom of Information Act 2000, the Data Protection Act 2018 and good records management.

All persons employed or engaged by HEIW should have appropriate training before being given access to systems.

Line managers are responsible for ensuring that relevant policies are brought to their staff attention during the local induction stage (i.e. staff induction manager's checklist) and new user authorisation process.

15. Sharing of Information

The HEIW will conform to the Wales Accord for the Sharing of Personal Information (WASPI) where the sharing and disclosure of person identifiable information is conducted on a regular basis.

Ad Hoc disclosures and communication methods considered appropriate for sharing will be subject to risk assessment.

16. Equality

In accordance with the HEIW 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, carers status, offending background or any other personal characteristic.

17. Monitoring and Enforcement of the Policy

Compliance with this policy will be monitored by the relevant Information Security team and IT departments within the HEIW.

HEIW will conduct regular audits to monitor compliance with this policy. Failure to comply may result in disciplinary action or even prosecution.

18. Contacts

A copy of this policy and other policies and procedures referenced in this statement are available on the HEIW's Intranet site. Contact details for the IT Service Desk, IT Training and Information Security staff/trainee can also be found on the Intranet site.

19. Further Information

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

- Information Governance Policy
- Data Protection & Confidentiality Policy
- Freedom of Information Act Policy
- Records Management Policy
- Email Policy
- Anti-virus Policy
- Internet Access Policy
- Software Policy

In addition there will be underlying Divisional policies, protocols and procedures to implement and support the HEIW wide policies.

20. Policy Review

This policy is valid for 3 years but will be reviewed on an annual basis.