DATA PROTECTION & CONFIDENTIALITY POLICY

Executive Sponsor & Function:

Board Secretary

Document Author:

Deputy Director Planning, Performance & Digital

Approved by:

Executive Team

Approval Date:

15 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

DATA PROTECTION & CONFIDENTIALITY POLICY

Overview:	This policy sets out the key areas of responsibilities and HEIW's commitment to ensuring the organisation treats all personal data lawfully and correctly.
Who is the policy intended	All persons employed or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts.
Key Messages included within the policy:	• Key principles to comply with Data Protection legislation • Framework covered to ensure all personal data is acquired, stored, processed and transferred in accordance with associated legislation. • Managing Subject access requests • Responsibilities of key personnel within HEIW
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

Health Education and Improvement Wales (HEIW) regard the lawful and correct processing of personal data (including staff/trainees) by HEIW as vital for maintaining confidence between those with whom the HEIW deal with. HEIW shall take all reasonable steps to ensure that it treats all personal data in accordance with this Policy.

This Policy sets out the high-level intent of HEIW.

2. Purpose

The purpose of this Policy is to set out the key areas of responsibilities and HEIW's commitment to ensuring the organisation treats all personal data lawfully and correctly.

For the purposes of this Policy HEIW takes the view that the principles of confidentiality apply to all personal data, held on computer or held manually and whether communicated verbally, electronically or in writing.

3. Scope of this Policy

This Policy applies to all personal data being processed within HEIW and its directorates regardless of how the data is being accessed, created, handled, received and/or stored.

4. Responsibilities

The policy applies to everyone working for or engaged by HEIW.

The **Chief Executive** of HEIW has overall responsibility for ensuring compliance with applicable legislation and regulation.

HEIW has a legal obligation to appoint a **Data Protection Officer**, whose role will be to undertake tasks to ensure that all personal data is being processed in accordance with this Policy and Data Protection Legislation. In HEIW this will be the Board Secretary.

NHS Standards stipulate the HEIW is required to have in place identified "**Caldicott Guardians**" with responsibilities for agreeing and monitoring protocols, and the movement and approval of the uses of patient and donor data within and external to HEIW. Although HEIW does not deal with patient information it has agreed this role shall be held by the Medical Director.

Everyone working for or engaged by HEIW are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data. Staff must adhere to all confidentiality requirements as described by HEIW and ensure that any access and use of personal data is only ever for the purposes of fulfilling NHS duties.

5. Further Information

5.1 Reporting of Data Protection & Confidentiality Breaches

HEIW takes any potential breach of Data Protection Legislation and confidentiality very seriously. All staff/trainees have a responsibility to report any breach of this nature immediately to the SIRO.

5.2 Training and Awareness

HEIW will ensure that adequate training is provided for all employees involved with processing of personal data and that qualified expertise is available for consultation. All new starters (to include Non-contract staff and those on short fixed term contracts) to HEIW will be given Information Governance training, to include compliance with Data Protection Legislation and general IT security training, as part of the HEIW induction process.

5.3 Contracts of Employment

All contracts of employment must include a data protection and general confidentiality clause. Agency, contractors and non-contract staff working on behalf of HEIW should be subject to the same rules.

5.4 Information, Transfer and Security

The use of telecommunication methods [i.e. post, fax, email, video/telephony, electronic] and/or data transportation methods [i.e. offsite transfer, laptops, USB sticks, CDs] as a means to transfer and communicate personal data without the appropriate controls being applied is regarded by HEIW as an insecure method of transferring confidential information.

Everyone working in or engaged by HEIW must pay particular attention with any need to transfer and communicate personal data via any form of telecommunication and/or data transportation methods, and HEIW expects this type of information to be communicated with care.

It is the responsibility of all members of staff, and in accordance with HEIW Policies to exercise their judgement to ensure suitable precautions are being applied to the transmission of all personal data.

5.5 Misdirection

Misdirection is the term associated with the accidental sending of personal data via methods to include emails, letters and faxes. Irrespective of whether or not the sending of personal data is sent internally or externally; misdirection is one of the main risks to HEIW. Accidental misdirection may result in a breach of confidentiality if the content identifies staff/trainee members.

In accordance with HEIW Policies to, **all** staff must ensure that appropriate protection and security measures are taken, to protect against unlawful or unauthorised disclosure of personal data, when there is a need to covey any personal data to internal or external parties'.

All persons employed or engaged must ensure that the correct recipient details are always selected to avoid the potential consequences of misdirection and/or accidental disclosure of personal data.

5.6 Social Media

Social media is a term for websites based on user participation and user-generated content. These media provide a number of benefits for HEIW as they are recognised as a valuable tool and provide another platform in which to engage with service users, to promote HEIW. It is the responsibility of all persons employed or engaged by HEIW to comply with HEIW's **Social Media Policy**.

5.7 Information Sharing

Such sharing may take place between the public services as well as appropriate private and third sector service providers. Sharing must take place legally, safely and with confidence in order to ensure public services are maintained and in order to improve standards and efficiency.

The Wales Accord for the Sharing of Personal Information (WASPI) is a framework under which information sharing protocols are formed where a regular sharing of personal data is to take place. HEIW has 'signed up' to use this framework and therefore in all instances of regular information sharing an Information Sharing Protocol should be adopted using the WASPI model.

5.8. Subject Access Requests

Data Protection Legislation establishes a framework of rights and duties that are designed to safeguard personal data. Individuals (known as data subjects) or their representatives, have a right to apply for access to information held about them, and in some cases, information held about others.

This is known as a Subject Access Request (SAR) and request for information must be made in writing. The SIRO will ensure that all requests are handled appropriately, and in accordance with Data Protection Legislation

5.9 Charging

Information is provided **free of charge**. However, HEIW can charge a 'reasonable fee' when a SAR is manifestly unfounded or excessive, particularly if it is repetitive.

Charging a reasonable fee can be applied to requests for further copies of the same information. However, it does not mean a charge can be applied to all subsequent access requests. Fees are to be charged based on the administrative cost of providing the information.

5.10 Time Compliance

Information must be provided without delay and at the latest within **30 days** of receipt. Where requests are complex or numerous, HEIW can extend the period of compliance by a further two months. If this is the case, respective organisations **must** inform the individual within one month of the receipt of the request and explain why the extension is necessary.

5.11 Appeal Process

If an individual believes that HEIW has not complied with this Policy or acted otherwise than in accordance with Data Protection Legislation, the individual has a right to refer their concerns to the ICO. However, in the first instance individuals should be offered the right to an internal review. This will be managed by the SIRO.

6. Available Guidance

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

Links to the ICO website also provide a valuable source of information.

7. Further Information

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

- 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