Ref: IG02

DATA PROTECTION & CONFIDENTIALITY POLICY

Executive Sponsor & Function:	Executive Director of Finance
Document Author:	Head of Information Governance
Approved by:	Quality, Safety and Performance Committee
Approval Date:	11 September 2025
Date of Equality Impact Assessment:	June 2025
Equality Impact Assessment Outcome:	Approved. No negative impact identified
Review Date:	September 2028
Version:	3

Contents **Page**

1. Aim **4**

2. Policy Statement and Objectives **4**

3. Scope of this Policy **4**

4. Data Protection and Confidentiality - Legislation and Standards **4**

4.1 Overview of Data Protection Legislation
4.1.1 Personal Data
4.1.2 Processing of Personal Data
4.1.3 Special Categories of Personal Data
4.1.4 The Principles
4.2 Information Security
4.3 Encryption
4.4 Closed Circuit Television (CCTV)
4.4.1 Processing of Images
4.5 Information, Transfer and Security
4.6 Misdirection
4.7 Social Media
4.8 Information Sharing
4.9 Monitoring/Auditing access to Personal Identifiable Data

5. Subject Access Requests **9**

5.1 Charging
5.2 Time Compliance
5.3 Appeal Process

6. Roles and Responsibilities **10**

6.1 Managerial Accountability and Responsibility
6.2 Reporting of Data Protection & Confidentiality Breaches
6.3 Contracts of Employment
6.4 Procurement

7. Breaches of this Policy **12**

8. Training, Awareness and Practical Considerations **12**

8.1 Training
8.2 Awareness
8.3 Practical Considerations

9. Complaints **14**

10. Governance and Reporting **14**

11. References – Specific applicable Legislation and Standards **15**

12. Equality **16**

13. Contacts **16**

14. Further Information **16**

1. AIM

The aim of this Policy is to set out the key areas of responsibilities and the Trusts commitment to ensuring the organisation treats all personal data lawfully and correctly.

For the purposes of this Policy, the Trust takes the view that the principles of confidentiality apply to all personal data, whether employee, patient, donor and/or service user held on computer or held manually and whether communicated verbally, electronically or in writing.

The policy also aims to provide all employees of the Trust with a framework in which to ensure that processing of all data is dealt with lawfully and in conjunction with this policy.

2. POLICY STATEMENT AND OBJECTIVES

Velindre University NHS Trust (the Trust) regard the lawful and correct processing of personal data (including patient, donor and staff) by the Trust as vital for maintaining confidence between those with whom the Trust deal and itself. The Trust 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 the Trust and recognises the diversity of the respective Divisions and associated organisations under its control.

3. SCOPE OF THIS POLICY

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

4. DATA PROTECTION AND CONFIDENTIALITY – LEGISLATION AND STANDARDS

This Policy provides all employees of the Trust with a framework to ensure all personal data is acquired, stored, processed and transferred in accordance with associated legislation, namely Data Protection Legislation, NHS standards [i.e. Caldicott Principles], and associated guidance issued by UK Government, Department of Health, Welsh Government, Information Commissioners Office (ICO) and other professional bodies.

4.1 Overview of Data Protection Legislation

Data Protection Legislation is about the rights and freedoms of living individuals, and particularly their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and concise about why personal data is being collected, and how the data is going to be used, stored and shared. The most common way to provide this information is in a Privacy Notice.

4.1.1 Personal Data

The definition of Personal Data within the Data Protection Act 2018 is: Any information relating to an identified or identifiable natural person (Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In practical terms it may include information necessary for employment such as staff member's names and addresses and details for payment of salary or a patient/donor record. Personal data may also include what is termed as special categories of personal data which is defined further in Section 4.1.3.

4.1.2 Processing of Personal Data

The processing of personal data is lawful only if ONE of the following six lawful bases of processing of personal data applies:

- The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller (The Trust) is subject;
- Processing is necessary to protect the vital interests of the Data Subject or another natural person (to safeguard life)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller (The Trust)
- Processing is necessary for the purposes of the legitimate interests pursued by the Controller (The Trust) or by a third Party (Processor as defined in Data Protection Law), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential. In accordance with The Data Protection Act, all personal data should only be processed in accordance with the six lawful bases for processing, on a need to know basis and all outputs must be treated carefully and disposed of in a secure manner. Staff must not disclose personal data outside their line of duty without a justified and lawful reason.

4.1.3 Special Categories of Personal Data

The Trust and its respective divisions and hosted organisations will, at times, be required to process special categories of personal data. Special category Personal Data is defined in the Data Protection Act as the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose

of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.1.4 The Seven Principles

The Trust shall comply with Data Protection Principles contained within the Data Protection Act 2018 in that Personal Data shall be: -

- Lawfully, Fairly and Transparently processed
- Collected for specified, explicit and legitimate purposes and not processed further in a manner that is incompatible with these purposes
- Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed
- Accurate and where necessary kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data including protection against unlawful or unauthorized processing and against accidental loss, destruction or damage using appropriate technical and organizational measures

The Seventh (7th) Data Protection principle is accountability, the Trust is accountable for the personal data it processes, likewise all Staff employed by the Trust whether they are employees, students, volunteers or contractors are personally accountable for the personal data that they process.

4.2 Information Security

The Trust will take appropriate technical and organisational steps to ensure the security of personal data and manage the risks from internal and external threats.

The Trust will promote good security practice and awareness. All staff working for and/or on behalf of the Trust will use the NHS Wales computer and respective Trust network(s) [i.e. the Public Sector Broadband Aggregation (PSBA)] responsibly and will comply with the Trust Information Security policy together with relevant divisional/associated organisational directions and guidance.

All personal data stored within the Trust must have the appropriate safeguards and systems in place that protects against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage of personal data.

4.3 Encryption

Encryption technology is adopted within the Trust to adequately protect any personal data from unauthorised disclosure, whether by theft or accidental loss and minimising the impact of any inappropriate disclosure, whilst in transit or for those staff working offsite.

The Trust is fully committed to complying with relevant industry standards and NHS guidance in relation to a strong encryption strategy. Each division/associated organisation is to take responsibility for ensuring that all services have a sufficient encryption strategy in place to adequately mitigate the risk associated with each process.

4.4 Closed Circuit Television (CCTV)

CCTV cameras are situated across various Trust premises for the purposes of crime prevention and detection and to help improve the security for our staff, service users and visitors.

To comply with legislation and Surveillance Camera Code of Practice 2021, it is essential that the location of CCTV cameras is carefully considered to ensure they do not infringe on clinical/treatment areas. Where CCTV cameras are situated, signs must be erected indicating their presence and posted in prominent positions, ensuring all staff, visitors and service users are aware they are entering an area that is covered by CCTV cameras. These signs must also include details on the purpose, organisation and responsible officer's contact details.

4.4.1 Processing of Images

Images, which are not required for the purpose(s) for which the CCTV cameras are being used, should not be retained for longer than is necessary. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of Data Protection Legislation.

Where images are required for evidential purposes in legal or NHS disciplinary proceedings, the Trust reserves the right to make a Data Recording. Any data recordings taken must have appropriate encryption techniques considered and deployed. The Trust will take a considered approach to the taking of data recordings and any such recordings will only be conducted on the basis that there is a suspected breach of either an NHS Wales policy or legislation. On deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

4.5 Information, Transfer and Security

The use of telecommunication methods [i.e. post, fax, email, instant messaging, SMS Text and videotelephony] 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 the Trust as an insecure method of transferring confidential patient, donor and/or staff information.

Staff must pay particular attention with any need to transfer and communicate personal data via any form of telecommunication and/or data transportation methods, and the Trust expects this type of information to be communicated with care.

It is the responsibility of all members of staff, and in accordance with Trust Policies together with relevant divisional/associated organisational directions and guidance, to exercise their judgement to ensure suitable precautions are being applied to the transmission of all personal data.

The Digital Services department implement data loss prevention (DLP) and portable device control via Antivirus tools to manage the security of data transportation methods (as above). If you are still required to transport Trust data via the methods listed above, these must be encrypted.

The use of NCCCs (e.g. WhatsApp/Facebook Messenger) is prohibited for the processing of personal data of patients, Staff and Service Users for business purposes in all formats including imagery and voice unless permitted in limited circumstances by the Information Governance team.

4.6 Misdirection

Misdirection is the term associated with the accidental sending of personal data via methods to include emails, instant messaging, SMS, letters and faxes. Irrespective of whether the personal data is sent internally or externally; misdirection is one of the main risks to the Trust. Accidental misdirection may result in a breach of confidentiality if the content identifies patients, donors or staff members.

In accordance with Trust Policies together with relevant divisional/associated organisational directions and guidance, **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'.

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

4.7 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 the Trust as they are recognised as a valuable tool and provide another platform in which to engage with patients, donors and service users, to promote the Trust and its services. It is the responsibility of all members of staff to comply with the NHS Wales Social Media Policy.

4.8 Information Sharing

The Trust recognises the need to share personal data for the benefit of the users of the service. 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 to ensure public services are maintained and 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. The Trust 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.

Where personal data is to be shared as part of a commercial contract between the Trust and Suppliers, WASPI will not apply. In such circumstances, a Data Processing Agreement (sometimes known as a Data Sharing Agreement) may be required in addition to the Contract between the Trust and the Supplier. The Head of Information Governance is to be consulted at the beginning of the commercial relationship so that Data Protection requirements can be identified as early as possible within the

proposed project. This is known as Data Protection by Design and by Default and is a legal requirement.

4.9 Monitoring/Auditing access to Personal Identifiable Data

The Trust reserves the right to monitor/audit staff's access to personal data via Trust systems. The Trust will use appropriate system audit functionality (to include the National Intelligent Integrated Auditing Solution) to detect potential misuse of access rights whereby employees may have abused their access rights to view personal data that they may not be entitled to view.

Any employee who is found to have abused their access rights may be subject to the Trust's Disciplinary Policy.

5. 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 requests for information may be made verbally or in writing.

Where a request is made verbally, it may be because some disabled people find it difficult to communicate in writing and may therefore have difficulty making a SAR. The Trust has a legal duty to make reasonable adjustments for such a person if they wish to make a Subject Access Request.

Reasonable adjustments could include treating a verbal request for information as though it were a valid Subject Access Request. If the request is complex, The Trust is to document it in an accessible format and to send it to the disabled person to confirm the details of the request.

The Trust may have to respond in a particular format that is accessible to the disabled person, such as Braille, large print, email, or audio formats. If an individual thinks that the Trust has failed to make a reasonable adjustment, they may make a claim under the Equality Act 2010.

Information about making a claim is available from the Equality and Human Rights Commission.

Where a request is made to access the records for a deceased person's health record, then the Access to Health Records Act 1990 is applicable.

The respective divisional/associated organisational leads should be notified of all requests, as these personnel are responsible for ensuring that all requests are handled appropriately, and in accordance with Data Protection Legislation.

The Head of Information Governance is available to provide professional and technical advice/guidance relating to the SAR process should it be required.

5.1 Charging

Information is provided **free of charge**. However, the Trust, and its associated organisations 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.

5.2 Time Compliance

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

5.3 Appeal Process

If an individual believes that the Trust has not complied with this Policy or acted otherwise then 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 state a complaint. All complaints should be dealt with at the lowest level, therefore in many cases a complaint can be processed with support from the respective divisional/hosted organisational leads.

6. ROLES AND RESPONSIBILITIES

The policy applies to all employees and contractors working for, or on behalf of the Trust. 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.

6.1 Managerial Accountability and Responsibility

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

The Trust has a legal obligation to appoint a **Data Protection Officer**, whose role is to undertake tasks to ensure that all personal data is being processed in accordance with this Policy and Data Protection Legislation. The Head of Information Governance is the Trust's appointed Data Protection Officer.

Directors of Hosted Bodies and Divisions within the Trust are responsible for ensuring that the Policy is implemented within their individual organisation, and must ensure: -

- everyone managing and handling personal data understands they are contractually responsible for following good Data Protection and Caldicott practice;
- everyone managing and handling personal data is appropriately trained to do so; and

- methods of handling personal data are clearly described.

NHS Standards stipulate the Trust 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 the Trust. The Trust's Caldicott Guardians are as below for its divisions:

Velindre University NHS Trust – Medical Director
Velindre Cancer Service – Clinical Director
Welsh Blood Service – Medical Director

The Trust has dedicated **Information Governance champions** in respective divisions and Hosted Bodies. These roles act as a first contact for receiving Data Protection queries and act as an advisor to other managers and employees within their respective areas.

Digital System managers responsible for the major information and clinical systems throughout the Trust will ensure that their systems meet the specifics within the data protection notification. They will also be responsible for notifying the respective leads within their organisation, of any changes to their system which may impact on Data Protection.

All staff 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 the Trust and ensure that any access and use of personal data is only ever for the purposes of fulfilling NHS duties.

Any employee who is found to compromise security or confidentiality of the Trust, its patients, donors, staff and/or service user's personal data may be subject to Trust Disciplinary Policy.

6.2 Reporting of Data Protection & Confidentiality Breaches

The Trust takes any potential breach of Data Protection Legislation and confidentiality very seriously. All staff have a responsibility to report any breach of this nature immediately. The Trust, divisions and associated organisations must have a mechanism for reporting incidents and these must be investigated in line with local procedures. Any reporting must be made in conjunction with the Trust Confidentiality Breach Reporting Policy. Staff not reporting incidents of this nature may be subject to the Trust's disciplinary policy.

6.3 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 the Trust are subject to the same rules, these clauses must be outlined in any honorary contract agreements issued prior to commencing work with the Trust.

6.4 Procurement

When considering procuring platforms that will by their very nature process personal data, the Head of Information Governance is to be consulted at the outset of the proposed project, this is because a risk assessment will need to be undertaken to assess the risk to the rights and freedoms of individuals known as Data Subjects. This process is called a Data Protection Impact Assessment.

It is a legal requirement to undertake this activity when;

- The proposed platform is new, novel or involves processing of large amounts of personal data

It is also considered to be best practice for other projects involving the processing of personal data.

7. BREACHES OF THIS POLICY

Any suspected breaches of this Policy will be taken seriously and investigated through the Trust's Disciplinary Policy. Breaches of data protection and confidentiality could be a criminal offence and/or gross misconduct and may lead to dismissal.

8. TRAINING, AWARENESS AND PRACTICAL CONSIDERATIONS

The Trust demonstrates that employees understand their responsibilities to ensure that personal information is protected and processed in accordance with the applicable procedures, taking into account the related security requirements.

8.1 Training

The Trust will ensure that adequate training is provided for all staff involved with processing of personal data and that qualified expertise is available for consultation. All new starters (to include non-contracted staff and those on fixed term contracts) to the Trust will be given Information Governance awareness training upon appointment, to include compliance with Data Protection Legislation, Records Management and Cyber Security training, as part of the Trust induction process.

Refresher training must be undertaken every two years following initial completion of training.

8.2 Awareness

Situational awareness is a key requirement in ensuring that members of Staff comply with Data Protection Legislation. Examples of such awareness are:

- Data Protection and Information Governance Policies
- Caldicott Principles
- Being aware of their contribution to the effectiveness of data protection and information management policies, including the benefits of improved information management performance
- The implications of not conforming with the Trust's data protection and information management policies.

8.3 Practical Considerations

In a fast moving technological world, training and awareness are linked to the practical considerations that context provides. Trust employees are working in a way which is completely different to a "normal" way of working with more remote working than ever before. The following are considerations that members of Staff must think about when remote working in relation to Data Protection and Confidentiality:

- Removable media – Staff are only to work within the confines of Trust policies relating to the use of removable media, if a member of Staff is permitted to use it, they are to keep the removable media device secure at all times, they are personally responsible for its safekeeping.
- Home Wi-Fi – Member of Staff are to ensure that the password to their home Wi-Fi device is not the factory setting. The password should be set to one that is only known to them and difficult to guess.
- The Data Protection Act –Applies at all times, no matter where the member of Staff is located; Wales, the UK or indeed worldwide.
- Information – It is immaterial whether the information is hard copy or electronic, information is still to be protected at all times, as a member of Staff this responsibility is shared by all. This includes within the home – hard copy or electronic information is not to be left unattended and be available where it may be seen by unauthorised personnel (this includes family members).
- Situational Awareness – Staff are to be mindful of their locations in terms of where they are working, are they near a window which permits their screen to be seen, could they be overheard or is the work they are doing far too sensitive for their location (including at home)?If any of these apply, staff must either move position or if movement cannot be mitigated, the staff member should not attempt to carry out the work.
- Screen Sharing – When sharing a screen as part of video conferencing, staff are to be mindful of what other participants can see. They are to close all applications prior to the call – this includes e-mails, document folders, documents names, the list is not exhaustive
- Locking access to the electronic device – All staff should operate on a need-to-know basis, this includes access to information by colleagues and family members. To safeguard information, it is imperative that ctrl/alt/del is pressed to lock the screen whenever the machine is not attended. It should be noted that most devices within the Trust are set to lock automatically at the 5 minute point, but within that 5 minutes, an intruder may be able to access information, presenting high risk to not only patient confidentiality but the individual's and the Trust's compliance with Data Protection Legislation. The way to protect information in this setting is to lock the screen immediately when the user steps away from their machine.

The Information Governance team are the professional source of advice and guidance for the Trust. Should a member of Staff have concerns or wish to raise any issues related to practical considerations, it is strongly recommended that they contact them prior to undertaking any activity.

Guidance on the procedures necessary to comply with this Policy should be made available from the respective divisions and associated organisations of the Trust or on its web pages. Managers will be responsible for ensuring that all their staff are made aware of Trust policies and standards.

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

9. COMPLAINTS

Anyone whose data is processed by the Trust is entitled to make a complaint if they are unhappy with the way their data has been processed.

Data Protection complaints are that same as any other complaint, however, the individual handling the complaint will be the Head of Information Governance who may need to undertake an investigation into the facts surrounding the complaint prior to responding to the complainant.

Members of Staff are to provide the following address for any individual who wishes to complain to the Trust about how their data has been handled:

Mr Ian Bevan via
VelindreInformationGovernance@wales.nhs.uk
Head of Information Governance
Velindre University NHS Trust
2, Charnwood Court
Heol Billingsley
Parc Nantgarw
Cardiff / Caerdydd
CF15 7QZ
Tel / Ffon - 029 20196161

It should be noted that an individual has the right not to complain to the Trust, but to the Information Commissioner's Office (ICO) by writing to:

Information Commissioner's Office – Wales
2nd Floor
Churchill House
Churchill Way
Cardiff
CF10 2HH

Tel: 0330 414 6421
Email: wales@ico.org.uk

10. GOVERNANCE AND REPORTING

Compliance with this policy (and supporting procedures) will be monitored by the Head of Information Governance. An internal audit on the Trust's arrangements in relation to the Act will be scheduled in line with the Trust's internal audit strategy.

For assurance, details on Data Protection and Confidentiality activity (including complaints) will be reported to the Quality, Safety and Performance Committee, as well as the Senior Information Risk Owner (SIRO).

An annual Caldicott review and audit will be carried out, by associated organisations within the Trust, in respect of the way patient and/or donor information is managed and recommendations for progress established.

The Trust 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 the Trust. 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 affected by major internal or external changes such as:

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

11. REFERENCES – SPECIFIC APPLICABLE LEGISLATION AND STANDARDS

This Policy is written in accordance with current legislation as well as relevant codes of practice and standards that include, but are not limited to, the following:

Human Rights

- European Convention on Human Rights
- Human Rights Act 1998

Rights to Privacy

- Investigatory Powers Act 2016
- Protection of Freedoms Act 2012
- Lawful Business Practice Regulations 2000

Data Protection

- Data Protection Act 2018 (incudes UK GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records Act 1990 (where not superseded by Data Protection Legislation)
- Health & Social Care Act 2012
- Data (Use and Access) Act 2025

Online Privacy

- UK Privacy and Electronic Communications Regulations (PECR)
- UK Privacy and Electronic Communications Amendment 2012 (Cookie Law)

Relevant Codes of Practice and Standards include, but are not limited to, the following:

- Caldicott Principles
- Information Security ISO27001
- Information Commissioners Codes of Practice
- ICO's Employment Information Guidance
- Common Law Duty of Confidence

12. EQUALITY

In accordance with the Trust'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.

As a result this policy will make reasonable adjustments for disabled people where they request their data under the Subject Access Request Process.

Further details are contained within Section 5 of this Policy.

13. CONTACTS

For further advice and/or assistance on how to ensure individual, divisional and associated organisational compliance with this Policy, please contact: -

Ian Bevan
Head of Information Governance
Velindre University NHS Trust HQ
2, Charnwood Court
Heol Billingsley
Parc Nantgarw
Cardiff
CF15 7QZ
Email – VelindreInformationGovernance@wales.nhs.uk

Tel – 029 2031 6161

14. FURTHER INFORMATION

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

- Information Governance Policy
- Confidentiality Breach Reporting Policy
- Records Management Policy
- Freedom of Information Act Policy
- Data Quality Policy
- Information Security Policy
- Email and Instant Messaging (EIM) Use Policy
- NHS Wales Internet Use Policy
- Social Media Policy