QMSIG06 Data Protection Policy	
VERSION:	15
DATE LAST UPDATED:	December 2021
REVIEW DATE:	December 2022
RELATED DOCUMENTS:	
OWNER / LEAD INDIVIDUAL:	**Owner / Lead Individual:** Chief Executive
DOCUMENT APPROVAL:	**Peer/Sub-Group:** Governance Committee
PATIENT ACCESS:	☺
SECURITY INFORMATION (PUBLIC, INTERNAL, CONFIDENTIAL):	Internal

Version Control Sheet

Policy Name:	Data Protection Policy	Policy Reference:	QMSIG06

Version	Date	Comment
01	Jan-14	New Policy
02	Jan-15	Reviewed and brought in line with current practice and amended policy references
03	Feb-15	Replaced all "should" statements with "shall" following risk assessment
04	Feb -16	Reviewed as a part of desktop audit, no changes.
05	May-16	New Reviewer/ Lead Individual due to changes in the hospital's structure, ISM/SMT Group added
06	May- 17	Reviewed, no changes
07	Jan - 18	Update for titles related to organisational change.
08	May-18	Reviewed in line with the new legislation: Data Protection Act 2018, GDPR 2016/679
09	July-18	DPIA Flow chart has been added
10	Feb-19	Section regarding Pseudonymisation has been extended, previously this was also cover within the classification policy (QMSIG03)
11	Apr-19	Minor Changes -Flowchart (DPIA) has been updated to include forms QMS numbers.
12	July-2020	Changes due to a new hospital structure, policy has been re-assigned
13	Nov-19	Full annual review. Changes in the line with hospital's new governance structure.
14	Dec-20	Full annual review.
15	Dec-21	Annual Review – no changes made

1. Purpose, Scope and Users

Cheswold Park Hospital (CPH) recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information governance plays a key part in the delivery of clinical governance, service planning and performance management.

The lawful and correct treatment of personal data is vital to maintaining confidentiality within the Hospital. Therefore, the Hospital will, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the General Data Protection Regulation and Data Protection Act 2018.
- take appropriate technical and organisational security measures to safeguard personal data;

This policy covers information held and processed by Cheswold Park Hospital. The Hospital is responsible for its own information under the terms of the Data Protection Act 2018, and it has a registration with the Information Commissioner Office which is renewed annually.

The information and guidelines within this policy are important and apply to all full-time and part-time employees of the organisation, and to non-executive directors, contracted third parties (including agency staff), locums, students and trainees, secondees and other staff on temporary placements with the organisation, and staff of partner organisations with approved access; other individuals and agencies who may gain access to data, such as volunteers, visiting professionals or researchers, and companies providing IT services to the organisation.

2. Reference Documents

Effective Information Governance is derived from legal requirements, central guidance and best practice in information handling, including:

- Data Protection Act 2018
- Freedom of Information Act 2000
- Caldicott Review Principles
- EU GDPR 2016/679
- The common law duty of confidentiality
- Environmental Information Regulations
- QMSIG01 Information Governance
- QMSIG10 Data Breach Response and Notification Procedure
- QMSIT01 Computer Acceptable Use Policy
- QMSIG04 Closed Circuit Television (CCTV) Policy

This Data Protection Policy shall therefore be considered as a key aspect of an overarching framework for the local delivery of Information Governance at Cheswold Park Hospital.

3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

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

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymisation: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymised data is still personal data, the processing of pseudonymised data should comply with the Personal Data Processing principles.

4. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

A. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

B. Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

C. Data Minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The organisation must apply anonymization or pseudonymisation to personal data if possible to reduce the risks to the data subjects concerned.

D. Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

E. Storage Period Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

F. Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Company must use appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

G. Accountability

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

5. Building Data Protection into Cheswold park Hospital Activities

In order to demonstrate compliance with the principles of data protection, an organisation should build data protection into its business activities.

5.1 Collection

If personal data is collected from a third party, the person collecting the data must ensure that the personal data is collected lawfully. If they are unsure, they must seek clarification with Data Protection Officer/ Head of department.

5.2 Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of personal data must be consistent with the information contained in the Privacy Notice. The Hospital must maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. Chief Executive is responsible for compliance with the requirements listed in this section.

5.2 Third-party supplier, business partners and data processors

Whenever the Hospital uses a third-party supplier or business partner to process personal data on its behalf, Director of Business Information & Systems (Deputy SIRO) must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks. For any other suppliers, which main purpose is not to process data, or provide a system processing data, e.g. contractors working on site, this responsibility sits with the Facilities Manager.

The Hospital must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards the Hospital or upon the instructions of the Hospital and not for any other purposes. When the Hospital processes personal data jointly with an independent third party, the Hospital must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

5.3 Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards must be used including the signing of a Data Transfer Agreement, as required by the European Union and, if required, authorization from the relevant Data Protection Authority must be obtained.

5.4 Rights of Access by Data Subject

When acting as a data controller, Data Protection Officer is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure.

5.4 Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. Data Protection Officer is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals.

5.5 Right to be forgotten

Upon request, Data Subjects have the right to obtain from the Company the erasure of its personal data. When the Company is acting as a Controller, Data Protection Officer must take necessary actions (including technical measures) to inform the third parties who use or process that data to comply with the

request. ***The right is not absolute and only applies in certain circumstances,*** for example when:

- the personal data is no longer necessary for the purpose which the data controller originally collected or processed it for;
- the data controller is relying on consent as lawful basis for holding the data, and the individual withdraws their consent; (e.g. staff member or a patient had consented for a photograph to be taken and displayed in the hospital, however later the consent was withdrawn)

5.6 Data Protection Impact assessment

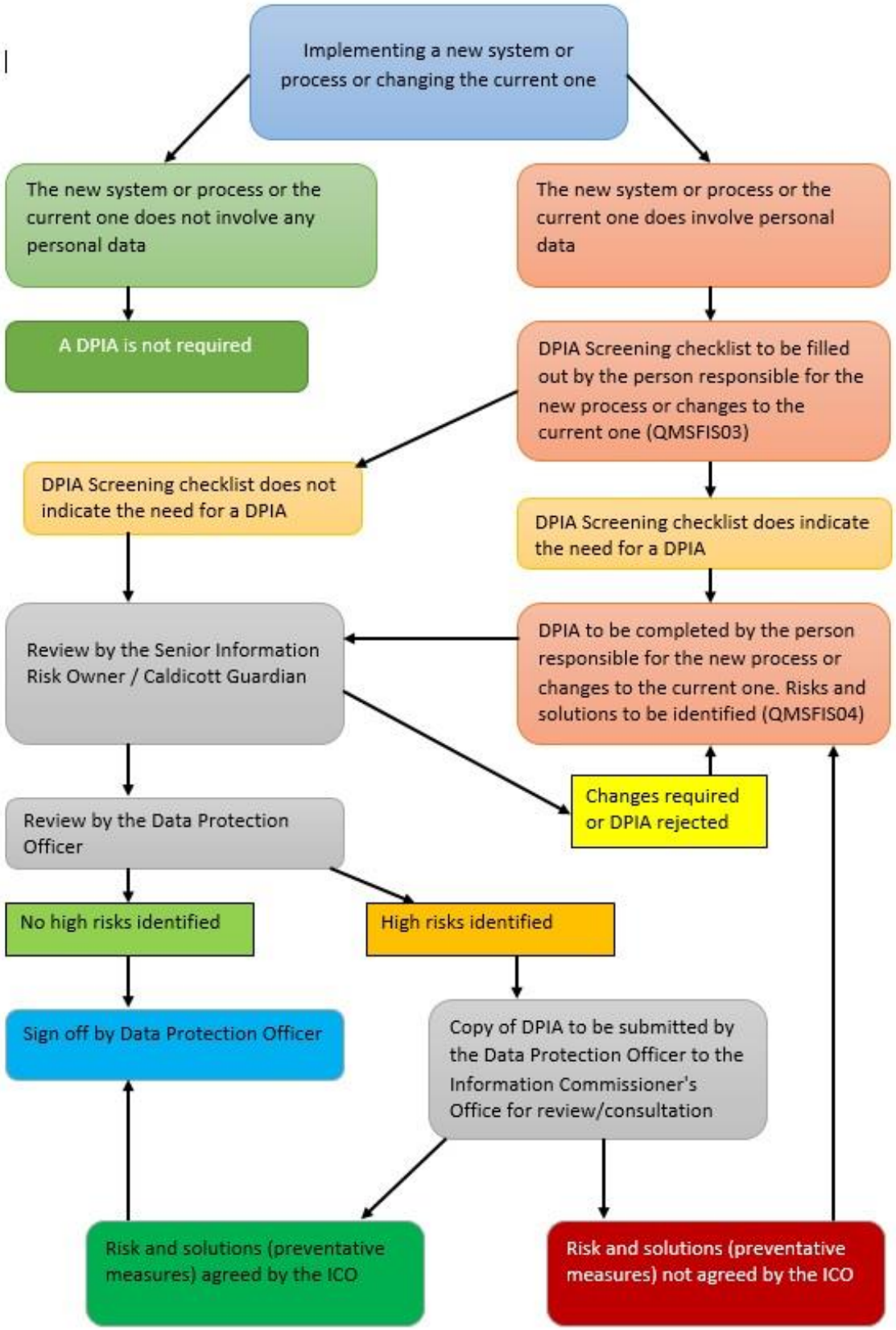
Data Protection Impact assessment is mandatory for data controllers for processing that is likely to result in a high risk to individuals. Where significant parts of the processing take place with the processor, the processor must assist with the DPIA at the request of the controller.
DPIA must be done prior to processing of personal data. Steps required are as follow:

A. When implementing a new system or process or changing the current one a person responsible for each data processing activity must determine if the activity involves any personal data. If the person responsible answer 'Yes' to this question, a DPIA screening checklist must be completed (available on the QMS: QMSFIS03)

B. If DPIA indicates the need for a DPIA the person responsible for the new process or changes to the current one must complete a full Data Protection Impact Assessment (document reference number QMSFIS04). Findings must be used to identify and list key security risks associated with the processing activity in question, and a mitigation plan must be formulated. Data Protection Officer may be consulted.

C. Completed DPIA must be sent to the SIRO/Caldicott Guardian for review, if DPIA is accepted SIRO/Caldicott Guardian will send it off to a Data Protection Officer.

D. If the results of the DPIA indicate that data processing activity would result in a high risk even if the security measures are implemented, then the Data Protection Officer must consult the supervisory authority before the data processing takes place.


Implementing a new system or process or changing the current one
The new system or process or the current one does not involve any personal data
The new system or process or the current one does involve personal data
A DPIA is not required
DPIA Screening checklist to be filled out by the person responsible for the new process or changes to the current one (QMSFIS03)
DPIA Screening checklist does not indicate the need for a DPIA
DPIA Screening checklist does indicate the need for a DPIA
Review by the Senior Information Risk Owner / Caldicott Guardian
DPIA to be completed by the person responsible for the new process or changes to the current one. Risks and solutions to be identified (QMSFIS04)
Changes required or DPIA rejected
Review by the Data Protection Officer
No high risks identified
High risks identified
Sign off by Data Protection Officer
Copy of DPIA to be submitted by the Data Protection Officer to the Information Commissioner's Office for review/consultation
Risk and solutions (preventative measures) agreed by the ICO
Risk and solutions (preventative measures) not agreed by the ICO

5.7 Data Protection by design and default

The GDPR/DPA 2018 makes data protection by design and default a legal requirement. The legislation requires the organisation to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This approach builds up on a privacy by design that had previously been adopted by the Hospital. Articles 25(1) and 25(2) of the GDPR outline obligations concerning data protection by design and by default. The first one says that:
"the controller shall, (…), implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'"
The second article states:
"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."
Cheswold Park Hospital (CPH) recognises the importance of the above, and:

A. Adopts an approach that ensures considering privacy and data protection issues at the design phase of any system, service, or process and then throughout the lifecycle, for example when:
    - developing new IT systems
    - using personal data for new purposes
    - developing policies

The hospital will involve members of Governance Committee and seek advice from the Data Protection Officer to ensure that all aspect of data protection have been address.

B. Process only the data that is necessary to achieve the specific purpose.
C. Ensure that personal data is automatically protected in any system.

5.8 Anonymisation/Pseudonymisation/De-Identification

Staff only have access to the data that is necessary for the completion of activity which they are involved in. This is reflected in the Caldicott Principles: access should be on a need to know basis. The principle applies to the use of Patient Identifiable Information foe secondary or no-direct care purposes. By de-identification users are able to make use of patient level clinical data for a range of secondary purposes without having to access the identifiable data items.

The aim of de-identification is to obscure the identifiable data items within the person records sufficiently that the risk of potential identification of the subject or persons record is minimised to acceptable levels.
De-identification can be achieved by:

- Removing patient identifiers

- The use of identifier ranges, for example; value ranges instead of age
- By using a pseudonym.

If patient data is required the CPH number is the most secure form of identifiable data.

To effectively pseudonymise data the following actions must be taken:

- Each field of Patient Identifiable Data must have a unique pseudonym
- Pseudonyms to be used in place of CPH numbers and other fields must be of the same length and formatted to ensure readability. E.g. in order to replace CPH numbers in existing report formats, then the pseudonym shall generally be of the same field length but not of the same characters
- Pseudonymised data shall have the same security as Patient Identifiable Information

Mental Health Act Office conducts regular checks/ audits on CPA, MHT, MMH, Face Risk/HoNOS/ HCR20 reports to ensure if CPH number has been used instead of patient's full names.

6. Responsibilities, accountabilities and duties

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with the Hospital and has access to personal data processed by the Hospital.

6.1 The key areas of responsibilities

The key areas of responsibilities for processing personal data lie with the following organisational roles:

- ***The Board of Directors*** makes decisions about and approves the Hospital's general strategies on personal data protection.

- ***Chief Executive Officer*** has overall accountability and responsibility for Information Governance which encompass' the Data Protection Act 2018.

- ***Caldicott Guardian*** have a responsibility to ensure patient data is kept secure. The Hospital's Caldicott Guardian is Medical Director.

- ***Senior Information Risk Owner (SIRO and Deputy SIRO)*** acts as an advocate for information risk within the Hospital and has responsibility for the ongoing development of the Hospital's Risk Management programme for Information Governance and security. The Hospitals' SIRO is Chief Executive and Deputy SIRO is Director of Business Information & Systems.

- ***Quality and Data Protection Officer*** informs and provide advice to all members of staff regarding their obligation to comply with the provisions of the Data Protection Act and GDPR, monitors compliance, and maintains the necessary documentation. Quality and Data Protection Officer is responsible for improving all employees' awareness of user personal data protection and for providing appropriate training. The GDPR requires that the DPO operates independently and although it allows DPOs to fulfil other tasks, organisations are obliged to ensure that these do not result in a conflict of interests with the DPO duties. To ensure that level of independence the Caldicott Guardian (Medical Director) will have direct managerial responsibility for the Quality and Data Protection Officer, as far as the DPO's duties are considered.

- ***Director of Business Information & Systems -*** Whenever the Hospital uses a third-party supplier or business partner to process personal data on its behalf, Director of Business Information & Systems (Deputy SIRO) must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks.

- ***Facilities Manager*** is responsible for passing on personal data protection responsibilities to suppliers which main purpose is not to process data, or provide a system processing data, e.g. contractors working on site.

- ***Heads of Departments*** are responsible for updating local registers of personal data processing activities and informing Data Protection Officer about any changes. Whenever personal data processing is based on the data subject's consent, Heads of Departments are responsible for retaining a record of such consent and making it available to the Data Protection Officer.

- ***All employees*** are required to comply with Data Protection and related policies e.g. employees who record information, whether electronic or on paper, have a responsibility to ensure that the data is accurate and as complete as possible. All employees are responsible for ensuring the security of information and data which they access within their role.

6.2 Responsibilities of Individual Data Users

All employees of the Hospital who record and/or process Personal Identifiable Data in any form (called "Data Users" in this policy) must ensure that they comply with the requirements of the Data Protection Act 2018 (including the Data Protection Principles) and with the Hospital's Data Protection Policy (including any procedures and guidelines which may be issued from time to time). A breach of the 2018 Act and/or the Hospital's Data Protection Policy may result in disciplinary proceedings.

Consideration shall be given towards contacting the Data Protection Officer for advice concerning the following:

- development of a new computer system for processing personal data;
- when using an existing computer system to process personal data for a new purpose;
- when creating a new manual filing system containing personal data;
- when using an existing manual filing system containing personal data for a new purpose;
- when transferring Personal Identifiable Data outside the Hospital boundaries;
- sharing Person Identifiable Information with third parties.

6.3 Accuracy of Data

All staff are responsible for:

- checking that any personal data they provide to the Hospital in connection with their employment is accurate and up to date e.g. change of address. The Hospital cannot be held responsible for any errors unless the member of staff has informed the Hospital about them.
- checking that any patient, staff or other individual's information they handle and record is as accurate and up to date as possible.

6.4 Data Security and Disclosure

All staff within the Hospital are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the Data Protection Officer.

Personal data must be kept securely and examples of how this may be done will include:

- keeping the data locked in a filing cabinet, drawer or room; or
- if the data is electronic, ensuring that the data is stored on the Hospital's network, that all equipment giving access to this information has sufficient security measures applied, and that mobile devices holding personal data are encrypted and kept securely; or
- any other appropriate security measure.

7. Procedure and Implementation

7.1 Notification to the Information Commissioner

The Hospital has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Notification monitoring within the Hospital is carried out by the Governance Committee. Individual data subjects can obtain full details of the Hospital's data protection registration/notification with the Information Commissioner from the Governance Team or from the Information Commissioner's website (www.ico.gov.uk).

It is a criminal offence for any Hospital employee to knowingly or recklessly operate outside the descriptions contained in the Hospital's notification entry.

The Hospital's registration documents will be held by the Governance Team on behalf of the Hospital.

7.2 Processing

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

Prior to introduction of a new processing activity an authorisation from the Director responsible for the affected area/department must be obtained. The responsible Director will contact Data Protection Officer and jointly will decide whether to perform the Data Protection Impact Assessment for each new data processing activity according to the Data Protection Impact Assessment Guidelines.

7.3 Notices to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, Data Protection Officer is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the Company's security

measures to protect personal data. This information is provided through Privacy Notice.

Where sensitive personal data is being collected, the Data Protection Officer must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

7.4 Special Categories of Personal Data

The Hospital may process "Special Categories of Personal Data" relating to staff, patients and other individuals.

"Special Category of Personal Data " is information as to a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs or beliefs of a similar nature, trade union membership, physical or mental health condition, sex life or sexual orientation, genetic data, biometric data. For example, data relating to the ethnic origin of individuals may be processed for the purposes of equal opportunities monitoring or to identify any necessary dietary requirements and possible sources of financial assistance. Medical records need to be processed for the provision of healthcare and general welfare, to identify any necessary dietary and accommodation requirements and to assist in meeting the needs of individuals with disabilities. In certain circumstances, the Hospital may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations. Whenever special categories of personal data are being processed based on the data subject's consent the data controller will need to make sure that "explicit consent" has been obtain.

All staff will be aware of their responsibilities and obligations to respect patient confidentiality. In addition, all clinical staff are bound to follow existing Professional Ethical principles of confidence as set out by the various clinical bodies.

7.5 CCTV

A number of CCTV cameras are present on site across the Hospital these are in place in order to assist with security for staff, patients, other individuals and property. If you have any queries regarding the operation of or access to the CCTV system, please contact the Data Protection Officer or see the QMSIG04 Closed Circuit Television (CCTV) Policy.

7.6 Email

It is permissible and appropriate for the Hospital to keep records of internal communications, provided such records comply with the Data Protection principles.

However, all Hospital staff need to be aware that:

- The Data Protection Act 2018 applies to emails which contain personal data about individuals which are sent or received by Hospital staff;
- Subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the Hospital to locate the personal data in the emails; and
- The legislation applies to all emails from and to members of the Hospital which are sent and received for Hospital purposes.

7.7 Data Subjects' Consent

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, Head of Department / Manager is responsible for retaining a record of such consent and making it available to the Data Protection Officer. Head of Department / Manager is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

Where collection of personal data relates to a child under the age of 16, Head of Department / Manager must ensure that parental consent is given prior to the collection using the Parental Consent Form.

When requests to correct, amend or destroy personal data records, Data Protection Officer must ensure that these requests are handled within a reasonable time frame. Data Protection Officer must also record the requests and keep a log of these.

Personal data must only be processed for the purpose for which they were originally collected. In the event that the Hospital wants to process collected personal data for another purpose, the Hospital must seek the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s). The Data Protection Officer is responsible for complying with the rules in this paragraph.

Now and in the future, Data Protection Officer must ensure that collection methods are compliant with relevant law, good practices and industry standards.

Data Protection Officer is responsible for creating and maintaining a Register of the Privacy Notices.

7.8 The Rights of a Data Subject

The Data Protection Act gives rights to individuals in respect of personal data held about them by others. The rights are:

- **The Right to be informed** - Individuals have the right to be informed about the collection and use of their personal data;
- **The Right of access** - Individuals have the right to access their personal data;
- **The Right to rectification**- a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete;
- **The Right to erasure**- also known as 'the right to be forgotten', in certain circumstances individuals have the right to request that their personal data is being erased;
- **The Right to restrict processing**- in certain circumstances, individuals have the right to request the restriction of their personal data. When processing is restricted, data controller is permitted to store the personal data, but not use it.
- **The Right to data portability**-this right allows individuals to obtain and reuse their personal data for their own purposes across different services;
- **The Right to object** – in certain circumstances, individuals the right to object to the processing of their personal data;
- **Rights in relation to automated decision making and profiling**.

An individual who wishes to exercise his/her rights is asked to formally do this by contacting hospital's Data Protection Officer via email dpo@cheswoldparkhospital.co.uk or telephone: 01302762862.

8 Retention of Data

The Hospital will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which they will be destroyed. This will be done in accordance with the retention period as set out by the Department of Health and Hospital's retention policy (QMSIG14 Data Quality Policy).

9. Response to Personal Data Breach Incidents

When the Hospital learns of a suspected or actual personal data breach and there is any risk to the rights and freedoms of data subjects, the Hospital must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours. For detailed procedure please see QMSIG10 Data Breach Response and Notification Procedure.

10. Audit and Accountability

The Governance Department is responsible for auditing how well hospital's departments implement this Policy.
Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

11 Conclusion

The Hospital recognizes the need to ensure that appropriate policies, procedures and process are in place to meet the requirements of the Data Protection Act 2018 and associated legislation and guidance.

The Hospital is committed to:

- Ensuring that the Hospital's notification to the Information Commissioner is current and complete and that it is renewed annually.

- The provision of training, guidance, information and support for all staff working for, or on behalf of, the Hospital with regards to their responsibilities in relation to the Act and service users, carers and other members of staff.

- Having accessible, understanding, efficient and supportive processes in place to help individuals, or people acting on their behalf, to have access to records containing their personal data.

- Having systems in place to identify where and how the Hospital can improve its performance on Data Protection and associated Information Governance requirement.

IMPACT EQUALITY ASSESSMENT

Cheswold Park Hospital is committed to ensuring that as far as is reasonably practicable, the way we provide services for our patients, visitors and treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds.

1. Screening			
How relevant is this policy and its associated procedures to promoting equality and eliminating discrimination? (indicate in boxes below)			
	Not relevant	Partly relevant (state which parts)	Very relevant
Race/ethnic group	✓		
Disability[1]	✓		
Gender	✓		
Age	✓		
Sexual Orientation	✓		
Religion	✓		
Other (please state)			
2. Assessing Impact (to be completed where the policy and associated procedures has been determined as relevant in the screening process)			
Please specify, in the rows below, anything that you have included in this policy and its associated procedures to ensure that equality is promoted and that no-one will be unlawfully disadvantaged (discriminated against) as a result of this policy.			
Race/ethnic group			
Disability[1]			
Gender			
Age			
Sexual Orientation			
Religion			
Other (please state)			

[1] Disability covers physical, sensory and mental impairments which include mental illness and learning disability. Long term conditions such as cancer, HIV and Multiple Sclerosis are included and any other normal condition at the point at which it begins to have an impact on a person's capacity to carry out normal day to day activities.