1.0 Policy Statement: Data Protection Policy

The General Data Protection Regulation (GDPR) comes into force across the European Union on 25 May 2018 and will apply to the Trust as data controller, where we determine the purposes and means of processing personal data for both employees and patients, and also as data processors where we are responsible for processing personal data on behalf of another data controller. The below policy statement is designed to provide a high level declaration of the current position and the expectation in terms of compliance with the GDPR.

The GDPR represents a step change in the way that data is protected and managed and will be supplemented by the yet to be passed Data Protection Act 2018. GDPR introduces new rights for data subjects and strengthens existing rights available under previous laws.

The Trust has established a GDPR working group to address the changes and ensure compliance, with leads for specific work streams across various disciplines. This work is overseen by the chair who is also the Trust Caldicott Guardian.

This policy covers all aspects of information within the Trust, including but not limited to:

- Personnel information
- Patient/client/service user information
- Staff/ students/ trainee/ apprentices/ volunteers information
- Organisational information

1.1 Accountabilities

This Policy applies to the Trust and all its employees, whether they are on permanent, fixed term or temporary contracts, contractors, students and voluntary. It also applies to external contractors who are employed to carry out work on behalf of the Trust, whether this is a temporary or time limited capacity. 3rd parties will be notified of their duties in the terms and conditions of their contract. Each individual is responsible for ensuring that they comply with relevant legislation and guidance for protecting the data they use.

2.0 Legal basis for processing data

As a data controller the Trust must establish and publish the lawful basis that is relied on for processing personal data and data that is special categories (sensitive data). The following table indicates for the main processing legal basis that the Trust is relying on for processing activities. Every service processing personal or special category data must ensure they document (via an asset register) and communicate (via a fair processing notice – see section 4.1 Transparency below) which lawful basis they are relying to process data.

The GDPR sets out conditions for lawful processing of personal data (Article 6) and further conditions for processing special categories of personal data (Article 9) as

listed in the table. If you are processing data relating to criminal convictions an Article 10 provision must also be satisfied.

3.0 Consent (Explicit consent)

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance reputation.

The GDPR definition of consent in Article 4(11) requires that:

- Consent must be given by a statement or by a clear affirmative action, and
- Consent must be freely given, specific, informed and unambiguous.

Only where there is no valid lawful basis to process data under GDPR then, individual's consent must be sought. Consent should not be used if a valid lawful basis exists.

Whilst consent may not be relied on for processing, there is still a requirement to inform the individual about how their data is being used (see section 4.1 transparency).

3.1 Consent and the Common Law (Implied consent)

If consent is not required under GDPR because another lawful basis exists, consent is still necessary to comply with the requirement of common law duty of confidence (confidentiality).

Implied consent is not a satisfactory standard for data protection law, as explained in section (3.0) as it must be an explicit clear affirmative action.

However for the purposes of common law, implied consent may be relied upon. This is consent which is not expressly granted by a person, but rather implicitly granted by a person's actions and the facts and circumstances of a particular situation – such as attending the emergency department or a GP.

Where consent is used to allow the lawful processing under GDPR, the following controls and considerations MUST be put in place:

- The requirement to facilitate withdrawal of consent – it must be as easy to withdraw as to give consent. This is known as Opt Out.
- The requirement that the Trust must be able to demonstrate that consent has been obtained. Consider where consent is recorded and ensure consent is dated so it is understood when it was obtained.
- the availability of the following rights (see rights in section 4.0):
- the right to erasure (where the subject withdraws consent and there is no overriding legitimate grounds to continue processing the data)
- The right to data portability.

3.2 Expiry of consent

In general once an individual has given consent, that consent may remain valid for

an indefinite duration, unless the individual subsequently withdraws that consent. For the purpose of this policy the consent duration should be time limited to the specific 'piece of work' that is being proposed. It should be considered good practice to seek 'fresh' consent once the original piece of work is completed or there are significant changes in the circumstances of the individual or the work being undertaken.

3.3 Refusal and withdrawal of consent

If an individual makes a voluntary and informed decision to refuse consent for their personal information to be shared, this decision must be respected unless there are sound legal grounds for not doing so. An individual, having given their consent, is entitled at any time to subsequently withdraw that consent. Like refusals, their wishes must be respected unless there are sound legal grounds for not doing so. If an individual refuses or withdraws consent the consequences of doing so should be explained to them but care must be exercised not to place the person under any undue pressure.

4.0 Data Subject/ Individual Rights in relation to information

All rights that are listed below must be actioned within one month, unless stated otherwise. This can be extended by two months where the request for is complex. A fee cannot be charged for processing of the request unless stated otherwise in this policy or supporting polices.

A request can be received both verbally and in writing so processes must be in place to ensure request can be logged and processed within the stipulated timeframes, please follow links below to local polices for how this applies in practice.

4.1 Transparency and the 'Right to be informed' – privacy notice

Individuals have the right to be informed about the collection and use of their personal data. The right to be told is also commonly referred to as a fair processing or privacy notice and is one of the most important rights. Regardless of what other rights apply to processing, the right to be told is fundamental to all rights being assessable by an individual. Done correctly the 'right to be told' about how information relating to the data subject is processed, should facilitate the use of data rather than hinder is use.

4.1.1 Privacy Notice Content

The following information must be communicated in the form of a privacy notice:

- The name and contact details of the Trust
- The name and contact details of our representative (if applicable).
- The contact details of our data protection officer
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing, (see section 2.5).
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

4.1.2 When to communicate privacy notice information

This information must be provided to individuals at the time their personal data is collected. If personal data is obtained from other sources, such as another organisation, individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.

Link to privacy notice.

4.2 Right of Access to Information

Individuals have the right to access their personal data and supplementary information such as audit data or Metadata (data about the data). The right of access allows individuals to be aware of and verify the lawfulness of the processing.

As a minimum a data subject can make a subject access request and is entitled to receive in full:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see section 4.1).

Information must be provided within one month of receipt free of charge. However, a ‘reasonable fee’ can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. For more details on how to make a request and when these conditions apply refer to the following

4.3 Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Where the information in question has been disclosed to others, each recipient should be contacted to inform them of the rectification - unless this proves

impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients

4.4 Right to Erasure

The right to erasure is also known as the 'right to be forgotten' introduces a right for individuals to have personal data erased. A request for erasure can be made verbally or in writing, therefore processes should be put in place to ensure both types of request can be logged and monitored. The right to erasure is not an absolute right and should only apply in the following circumstances:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed;
- consent was the lawful basis for holding the data, and the individual withdraws their consent;
- legitimate interests was the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the data is processed for direct marketing purposes and the individual objects to that processing;
- the personal data has been processed unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- comply with a legal obligation; or
- the personal data is being processed to offer information society services to a child.

4.5 Right to Restrict Processing

The right to restriction allows an individual to request the restriction or suppression of their personal data. This right is closely linked with the right to rectify and the right to object. The right to restrict the processing of their personal data is not an absolute right and should apply in the following circumstances:

- the individual contests the accuracy of their personal data and the accuracy is being verified by the trust;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- the personal data is no longer needed in line with retention but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under section and you are considering whether your legitimate grounds override those of the individual.
- When processing is restricted, the personal data can still be stored, but cannot be further used or processed.

Where an applicant has made a request to **rectify (4.3)** or **object (4.7)** to processing of their data, then the individual may have a right to restrict processing whilst these

rights are being assessed, so they should be considered at the same time. As a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question

4.6 Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The process should allow for moving, copying or transfer of personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability is not an absolute right and only applies:

- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

Therefore for care purposes, where data is processed under a statutory legal basis, the right to data portability would not apply. However where data is processed under the performance of a contract, with the individuals consent or the processing involves automated means, this right should be facilitated.

4.7 Right to Object

The right to object to processing means that data should cease to be processed. Individuals have the right to object to processing of their data where:

- Processing is based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); See section 2.0 for legal basis for processing).
- It us used for direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics (this does not include statutory reporting).

4.8 Rights relating to Automated Decision Making and Profiling

This is the process of making a decision solely by automated means without any human involvement, usually via a computer algorithm or formula. Profiling is automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.

Examples of this include:

- Risk stratification of patients based on frequency if attendance
- A recruitment aptitude test which uses pre-programmed algorithms and criteria.

If any of these techniques are used the following must be complied with:

- Send individuals a link the privacy statement data has been indirectly.
- Explain how people can access details of the information used to create

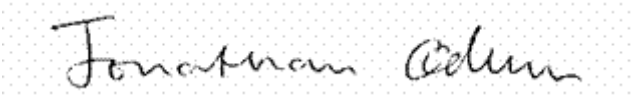
their profile.

- Tell individuals who provide their personal data how they can object to profiling, including profiling for marketing purposes.
- Have additional checks in place for profiling/automated decision-making systems to protect any vulnerable groups (including children).
- Only collect the minimum amount of data needed and have a clear retention policy for the profiles created

Staff must read this policy in conjunction with the existing IG policies that are available on the Trust Intranet page which will continue to apply until they have been updated.

Caldicott Guardian Signature

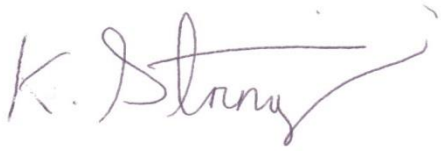
Dr. J Odum (Medical Director)



. . . . . .

Senior Information Risk Owner (SIRO) Signature

Kevin Stringer (Chief Financial Officer)



. . . . . .

Data Protection Officer Signature

Raz Edwards

. . . . . .

Legal basis for processing

Type of processing	GDPR Article 6 Condition for personal data	GDPR Article 9 Condition for special categories (sensitive data)	Statutory basis or other relevant conditions
Lawful basis for direct care and administrative purposes All health and adult social care providers are subject to the statutory duty to share information about a patient for their direct care. This would also include (a) preventive or occupational medicine, (b) the assessment of the working capacity of an employee, (c) medical diagnosis, (d) the provision of health care or treatment, (e) the provision of social care, or (f) the management of health care systems or services (g) waiting list management (h) performance against national targets (i) activity monitoring (j) local clinical audit	6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…' 6(1)(d) is available in life or death situations but should not be necessary for health or social care organisations to use in the performance of its tasks. This might apply in a situation where an organisation needs to act to prevent harm being caused by a patient or service user, to someone who has no relationship with the organisation.	NHS Trusts National Health Service and Community Care Act 1990 NHS England's powers to commission health services under the NHS Act 2006 or to delegate such powers 251B of the Health and Social Care Act 2012
Lawful basis for commissioning and planning purposes Most national and local flows of personal data in support of commissioning are established as collections by NHS Digital either centrally, or for local flows by its Data Services for Commissioners Regional Offices (DSCRO).	Where the collection or provision of data is a legal requirement, for example where NHS Digital is directed to collect specified data, and can require specified organisations to provide it, 6(1)(c) '…for compliance with a legal obligation…'	9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'	Commissioners may receive personal data in support of commissioning where confidentiality is set aside by provisions under the Control of Patient Information Regulations 2002, commonly known as 'section 251 support'. This support does not remove the need for GDPR compliance. The commissioning of individually tailored services, or for example the approval of individual funding requests should operate on the basis of consent for confidentiality purposes.
Lawful basis for research	6(1)(f)'…legitimate interests…except where such interests are overridden by the interests or	9(2)(j) '…scientific or historical research purposes or statistical purposes in accordance with Article	A pre-condition of applying Article 9(2)(j) is that the processing has a basis in UK (or EU) law. This basis will include compliance with the common

	fundamental rights and freedoms of the data subject…'	89(1) based on Union or member State law which shall be proportionate…and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject …'	law duty of confidence, the provisions of DPA18 that relate to research, statistical purposes etc. and other relevant legislation, for example section 251 support.
Lawful basis for regulatory and public health functions Processing that is necessary for reasons of public interest in the area of public health, and is carried out (i) by or under the responsibility of a health professional, or (ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.	6(1)(c) '…necessary for compliance with a legal obligation…	9(2)(j) ' …necessary for reasons of public interest in the area of public health…or ensuring high standards of quality and safety of health care and of medicinal products or medical devices…	Health Protection (Notification) Regulations 2010 Public Health (Control of Disease) Act 1984, as amended by the Health and Social Care Act 2008
Lawful basis for safeguarding	6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law..'	Children Acts 1989 and 2004, and the Care Act 2014
Lawful basis for employment purposes	6(1)(b) 'For the performance of a contract to which the 'individual' is a party' Or 6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment…social protection law in so far as it is authorised by Union or Member State law..'	Safeguarding Vulnerable Groups Act 20069 as a basis for Disclosure and Barring Service (DBS) checks and other processing of such data