The Newcastle Upon Tyne Hospitals NHS Foundation Trust

Data Protection Policy

Version No.:	1.1
Effective From:	13 February 2019
Expiry Date:	24 May 2021
Date Ratified:	12 February 2019
Ratified By:	Information Governance Committee

1 Summary

The Data Protection Act 2018 ('the Act') gives effect in UK law to European General Data Protection Regulations (GDPR) The Regulations apply to all data controllers who process personal data. The Trust, as a Public Authority, is a Data Controller.

Essentially the Act does three things:

- It requires every data controller to inform the relevant national authority of its processing operations ('Notification')
- It obliges data controllers to comply with a code of conduct on data processing
- It creates a set of enforceable expectations for individuals concerning the processing of their personal data.

All Trust staff may have access to personal identifiable information about patients, their families or colleagues as part of their duties.
This policy defines the legal and ethical responsibilities surrounding access and use of the data.
All Trust staff must abide by the conditions of this policy.

2. Principles

2.1 The Trust is required by law to comply with the Data Protection Act 2018. It is the commitment of the Trust to ensure that every employee complies with this Act to ensure the confidentiality of any personal data processed by the Trust in whatever medium (i.e. electronic systems, manual filing system).

2.2 All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the Trust. This relates to roles that are reliant upon computer systems such as: patient administration, purchasing, invoicing and treatment planning. Recent legislation also regulates the use of manual records relating to patients, staff and others whose information may be held within the Trust.

2.3 The Trust needs to collect and use certain types of information about people with whom it deals in order to operate. These include current past and prospective patients/service users and employees, suppliers and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 2018

3 Aims

This Policy has been developed to provide guidance, assistance and awareness for Trust staff to ensure a standard, consistent compliance to processing (creation; storage; retention; accuracy; relevance; disclosure and disposal) of personal identifiable data.

4 Duties (roles and responsibilities)

4.1 Staff shall be familiar with all Trust policies covering data processing and shall not perform any action in breach of those policies that could render the Trust liable at law nor shall any member of staff process or use data in breach of Trust policies in such a way as to bring the Trust into disrepute.

4.2 CEO / Trust Board Responsibilities

The Chief Executive is responsible as Accounting Officer for ensuring that Trust is legally compliant with the Data Protection Act 2018

4.3 Senior Information Risk Owner

The Trust Secretary as Senior Information Risk Owner acts as an advocate for information risk on the Trust Board. In addition they provide written advice to the accounting officer on the content of the annual statement of internal control in regards to information risk.

4.4 Caldicott Guardian Responsibilities

The Caldicott Guardian has a strategic role which involves representing and championing confidentiality and information sharing requirements and issues at senior management level. In addition they actively support information sharing and advise on options for lawful and ethical processing of information.

The Caldicott Guardian is also responsible for assuring the Trust Board that Data Protection Policies and systems complying with the Data Protection Act are in

place, and that a suitably trained and experienced Data Protection Officer is identified and notified to the Information Commissioner's Office.

4.5 Data Protection Officer.

Providing expert advice in respect of the Data Protection Act to the Trust Board and its senior officers.
Ensure that the access and informed consent provisions of the Data Protection Act are met by means of procedures applied by Subject Access Teams
Ensuring that there are processes in place for risk assessment, compliance audits and reports to the Information Governance Committee in respect of Data Protection issues.

On a day-to-day basis the Data Protection Officer will in addition be responsible for the following:

- Ensuring that appropriate Data Protection Act notification is maintained for applicable organisation's systems and information.
- Dealing with enquires, from any source, in relation to the Data Protection Act; facilitating Data Subject Notices.
- Advising users of information systems, applications and networks on their responsibilities under the Data Protection Act, including Subject Access.
- Investigating or Reviewing Incident Reports in respect of possible breaches of the Act and agreeing the recommended actions as part of the Trust and NHS Digital Serious Incident Procedures.
- Liaising with external organisations on Data Protection Act matters.
- Promoting awareness and providing guidance and advice on the Data Protection Act as it applies within the organisation, and generally ensuring that the Trust fulfils its role as Data Controller.

4.6 Subject Access Team Responsibilities

Subject Access Teams (Medical Records & HR) are employed to process Subject Access Requests for patient health records. They will follow detailed procedures, referring any issues which require further direction to the Information Governance Officer.

5 Specific policy

5.1 The Trust will handle personal data in accordance with the Act by:

- Obtaining and processing personal data in such a way that recognises the conditions for fair processing, for compliance with a legal obligation to which the Trust is subject, and for the exercise of the Trust's statutory functions;
- Collecting and processing personal data on a 'need to know' basis, ensuring that it is fit for purpose, not excessive, is disposed of at a time appropriate for its purpose and that adequate steps are taken to ensure the accuracy and currency of data;
- Ensuring that for all personal data, appropriate technical and organisational measures are taken to prevent damage, loss or abuse;
- Ensuring that the movement of personal data is done in a lawful way – both inside and outside the organisation;
- Acknowledging the rights of individuals to whom the personal data relates and ensure that these rights may be exercised in accordance with the Act.
- Ensuring that the Information Commissioner is notified of all relevant processing and will conduct a periodic review and update of the register entries to ensure that they remain up to date;
- Ensuring that an active 'fair processing' framework is in place, through which patients and staff are informed about the kind of purposes for which information about them is collected, and the categories of people or organisation to which such personal information may be passed. Such a framework will ensure that an individual's consent to the use of their information is informed.

The Trust (through its Data Protection Officer) will inform the Office of the Information Commissioner of the types of processing it undertakes.

The Trust will provide:

- A description of Personal data being processed, and of the categories of data subject to which they relate;
- A description of the purposes for which the data are being / are to be processed; The source(s) from which the Trust intends to obtain the information
- A description of all recipients to whom the Trust intends or may disclose information to;
- Details of any processing outside the European Economic Area when the
- Processing without notification, and processing of a type not reflected in the notification, are both criminal offences. It is also a criminal offence for any Trust employee to knowingly or recklessly operate outside the descriptions contained in the Trust's notification entry

5.2 The Trust will apply the principles contained in the UK Data Protection Act 2018 and the overarching General Data Protection Legislation specifically around the areas of legal processing and the rights of individuals.

5.2.1 Subject Access

Subject access will be managed in line with the rights given to each individual by the Data Protection Act 2018 subject to i) below and other applicable exemptions Access will be provided through application to the Subject Access desk in respect of patients and third parties, the Director of Human Resources in respect of staff or the Data Protection Officer.

The Trust will ensure:

- All requests for subject access will be accepted in writing only.
- All requests will be responded to within 30 days from receipt of a valid request or, if later, within days of receipt of –

Information confirming identity / legitimacy of individual making the request / assisting in the location of relevant data.

A request will not be met in the absence of:

- Written request;
- Information confirming identity of the individual making the request / assisting in the location of data (where necessary)
- All requests for subject access will receive a reply even when data is not held about the individual concerned.
- Where Personal data has been requested, and its release is not covered by exemptions under the Act, a copy of the data held will be supplied to the requester;
- In the event of information in the copy being unintelligible a reasonable explanation will be given to the requester by an appropriate Trust employee;
- Where a subject access request has been met previously, additional requests for similar or identical access by the same person will only be met following a reasonable time lapse.
- In deciding a reasonable time lapse the following factors will be considered:

- The nature of the data;
- The purpose for which the data are processed;
- Frequency with which the data are altered.
- Where a subject access request would result in the disclosure of information relating to an individual other than the data subject the Trust will only comply with the request if:
    - The other individual has consented to disclosure of the information;
    - It is reasonable in all the circumstances to comply with the request without the consent of the other individual. In deciding reasonableness the Trust will give regard to:
    - Any duty of confidentiality owed to the other individual;
    - Steps taken to seek the consent of the other individual;

    - Capability of the other individual to give consent;
    - Refusal of consent by the other individual.
- When requests are made by or on behalf of children, the Trust will at all times work within the law relating to the legal capacity of children (i.e. the request must be in the interests of the child and not just the parents).
- Requests in respect of patients will be subject to Lead Health Professional assessment of the possible application of S.30

Subject access requests will be referred to the Data Protection Officer if the application of an exemption is being considered.

5.3 Data Subject Notices

Under the Act, data subjects have the right to send a notice to the Trust, asking the Trust (within a reasonable time) to stop processing their information. This is a 'data subject notice.'

The Trust will ensure.

- All data subject notices will be accepted in writing only.
- A valid notice will include –
    - Identification details of the data subject and a description of the personal data to which they refer;
    - The nature of the processing and whether it is the processing for a specified purpose or in a specified manner to which they object;
    - When the data subject requires the processing of the personal data to cease (this must be at the end of a period which is reasonable in all the circumstances), or that the data subject does not wish the Trust to begin processing their personal data;
    - That the processing of personal data for the purpose specified is causing or is likely to cause the data subject or another persona substantial damage or substantial distress, and that damage or distress would be unwarranted; and
    - The reason why the data subject believes that the processing is causing or is likely to cause them or another person unwarranted damage and/or distress. A data subject notice will not be met in the absence of this information; All data subject notices will be responded to within 28 days from receipt of a valid notice. The response will inform the data subject either that the Trust has complied with or intends to comply with the data subject notice; or the extent to which the Trust intends to comply, explain which parts of the notice are considered to be unjustified, and why.

Data subject notices will be facilitated by the Trust's Data Protection Officer, who will report on notices and their outcomes through the Trust's assurance

processes.

5.4 Data Protection complaints and/or enquiries

Complaints about the Trust's Data Protection procedures, and appeals against decisions not to supply exempt information, will be dealt with by the Director of Governance, who will deal with the complaint in accordance with the Trust's Complaints Policy and Procedure. General enquiries about the Data Protection Act will be dealt with through the Data Protection Officer. DPA Section 10 notices from data subjects in respect of the right to prevent processing likely to cause damage or distress will be addressed and responded to by the Data Protection Officer

6 Disciplinary process

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

7 Training

It is the responsibility of all staff to complete the annual mandatory information governance training.

8 Equality and diversity

The Trust is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds. This document has been appropriately assessed.

9 Monitoring and compliance

Standard / process / issue	***Monitoring and audit***			
	Method	***By***	***Committee***	***Frequency***
Data protection notification. Information and data protection toolkit	The Trust is subject to external review through the Information commissioners office. The Data protection and Security Toolkit is an annual nhs return ensuring compliance.	Information Governance & Security team	IG committee	Continuous process.

IT Security will use audit tools to regularly monitor device usage and encryption compliance. Suspected breaches will be investigated and reported to HR and the Caldicott Guardian.

11 Consultation and review

The Data protection Officer, Head of Information Governance & Security and SIRO are responsible for the review and amendment of this policy.

12 Implementation (including raising awareness)

Regular communications with staff including annual mandatory training.

13 references

- Caldicott Code of Conduct on Confidentiality
- Data Protection Act 2018
- Freedom of Information Act 2000
- NHS Code of Confidentiality.

14 Associated documentation

- Clinical Records Management Policy
- Disciplinary Policy / Procedure
- Freedom of Information Act Procedure
- Information Governance Policy
- Non-Health related Records and Documents Retention Schedules

The Newcastle upon Tyne Hospitals NHS Foundation Trust

Equality Analysis Form A

This form must be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

PART 1

1. **Assessment Date:** _24/05/18_____

2. **Name of policy / guidance/ strategy / service development / Investment plan/Board Paper**:

Data Protection Policy

3. **Name and designation of author:**

Richard Oliver Data Protection Manager

4. **Names & Designations of those involved in the impact analysis screening process:**

Matt Carney Head of IG

5. **Is this a:** Policy x Strategy □ Service □ Board Paper □

Is this: New x Revised

Who is affected: Employees x Service Users x Wider Community x

6. **What are the main aims, objectives of the document you are reviewing and what are the intended outcomes?**
(These can be cut and pasted from your policy)

Outlines Trust compliance with the European Data Protection Legislation .

7. Does this policy, strategy, or service have any equality implications? Yes □ No X

If No, state reasons and the information used to make this decision, please refer to paragraph 2.3 of the Equality Analysis Guidance before providing reasons:

The Policy has no equality issues as it outlines the processes and procedures applicable to all members of the public in relation to the management and use of their personal information.

8. Summary of evidence related to protected characteristics

Protected Characteristic	**Evidence** **What evidence do you have that the Trust is meeting the needs of people in all protected Groups related to the document you are reviewing–** please refer to the Equality Evidence within the resources section at the link below: http://nuth-vintranet1:8080/cms/SupportServices/EqualityDiversityHumanRights.aspx	**Does evidence/engagement highlight areas of direct or indirect discrimination?** For example differences in access or outcomes for people with protected characteristics	**Are there any opportunities to advance equality of opportunity or foster good relations**? If yes what steps will be taken? (by whom, completion date and review date)
Race / Ethnic origin (including gypsies and travellers)	**This policy relates to the legal requirements for managing personal data.**		
Sex (male/ female)	**This policy relates to the legal requirements for managing personal data regardless of sex**		
Religion and Belief	**This policy relates to the legal requirements for managing personal data regardless of religion.**		
Sexual orientation including lesbian, gay and bisexual people	**This policy relates to the legal requirements for managing personal data regardless of sexual orientation.**		
Age	**This policy relates to the legal requirements for managing personal data regardless of age.**		
Disability – learning difficulties, physical disability,	**This policy relates to the legal requirements for managing personal data regardless of and difficulties or disabilities.**		

sensory impairment and mental health. Consider the needs of carers in this section			
Gender Re-assignment	**This policy relates to the legal requirements for managing personal data and has no impact on any Gender re-assignment.**		
Marriage and Civil Partnership	**This policy relates to the legal requirements for managing personal data and has no impact on marriage or Civil partnerships.**		
Maternity / Pregnancy	**This policy relates to the legal requirements for managing personal data.**		

9. Are there any gaps in the evidence outlined above? If 'yes' how will these be rectified?

Section 8 is not applicable to this policy.. see response in 7

10. Engagement has taken place with people who have protected characteristics and will continue through the Equality Delivery System and the Equality Diversity and Human Rights Group. Please note you may require further engagement in respect of any significant changes to policies, new developments and or changes to service delivery. In such circumstances please contact the Equality and Diversity Lead or the Involvement and Equalities Officer.

Do you require further engagement No

11. Could the policy, strategy or service have a negative impact on human rights? (E.g. the right to respect for private and family life, the right to a fair hearing and the right to education?)

No

PART 2

Name of author:

Richard Oliver

Date of completion

30/05/18

(If any reader of this procedural document identifies a potential discriminatory impact that has not been identified, please refer to the Policy Author identified above, together with any suggestions for action required to avoid/reduce the impact.)