Oxford Health
NHS Foundation Trust

Policy control document

This ensures good version control and effective policy management. It must be completed before a policy can be uploaded to the intranet.

Policy Title	Data Protection Act 2018 Appropriate Policy Document (Statement of Compliance with Processing Special Category Personal Data)
Policy Number	**CORP30**
Author(s) **(Name and Title/Role)**	Mark Underwood, Head of Information Governance Laura Hamilton, Information Governance Manager

Approval History	
Name of Committee	**Date**
Quality Committee	14th July 2022
Committee which approved current version **Quality Committee**	**Date of approval for current version** **14th July 2022**

Date of next review (Month/Year)	**31st July 2025**

Chair of Approving Committee: Andrea Young

Signature:

Title: Non-Executive Director
Date: 07.09.2022

All policies are copy controlled. When a revision is issued previous versions will be withdrawn. An electronic copy of the current policy with be posted on the Trust Intranet.

Change control

Number of pages (excluding appendices): 10
Summary of Revisions: This is the first version of this policy.
Any change to code or merging with other policies
Consultation with: Information Management Group

Data Protection Act 2018 Appropriate Policy Document (Statement of Compliance with Processing Special Category Personal Data)

Policy Code CORP30

Version 1
Date of Approval 14th July 2022

Contents

1. Purpose of policy (aims and objectives)

This policy is required by the Data Protection Act (DPA) 2018, the UK General Data Protection Regulation (UK GDPR) 2020, and associated laws. The act outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions to cover these processing activities. The health data processed by the Trust is SC data. This policy complements our general record of processing under Article 30 of the UK GDPR and provides SC and CO data with further protection and accountability. This policy supplements the Trust privacy notice, staff privacy notice and Integrated Information Governance Policy.

2. Outline of policy

This policy covers:

- The specific legal requirement of the DPA 2018 that the policy fulfils.
- A description of the ways personal data (SC and CO) is used, and the lawful bases relied upon to do so.
- It defines the procedures for ensuring compliance with the principles of accountability, lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality (security).
- Records Management including retention periods and erasure.
- It covers SC and CO personal data held and processed, about patients and service users, carers, applicants, students, and staff (both present and past) and third parties. It includes pseudonymised data but not anonymised data. It applies to all personal data, whether held on premise, cloud, on a portable device or by third parties. It applies to information held electronically and on paper.
- This policy covers the Trust's requirements for data protection, whether it is the Data Controller or Data Processor, and where the Trust works in partnership with other organisation(s) as joint Data Controller, for example, to achieve seamless or integrated care for patients or service users.
- Under the Data Protection Act 2018, the Trust processes personal data for the performance of a task carried out in the public interest and in exercising official authority. Depending on particular purpose of processing personal data the Trust may adopt an alternative lawful basis for example, in the event of a life-or-death situation.

This policy is applicable to all Trust employees and workers, Non-Executive Directors, students, contractors and third parties who work for the Trust and who have access to Trust information assets.

Activity and Purpose	Lawful basis for processing
Direct Care Personal Data a) Identity (b) Contact (c) Special Categories Special Categories, health, ethnicity	All Health and Adult Social Care providers are subject to the statutory duty under Section 251B of the Health and Social Care Act 2012 to share personal data about patients for their direct care. UK GDPR Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. UK GDPR Article 9 (2) (h) Processing is necessary for the purposes of preventative or occupational medicine for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or management of heath or social cares systems and services on the basis of Union or Member State law or a contract with a health professional.
To respond to a request under the Freedom of Information Act, enquiries, complaints (a) Identity (b) Contact	UK GDPR Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. Comply with a legal or regulatory obligation
To respond to a request under Data Protection Act or the UK General Data Protection Regulation a) Identity (b) Contact (c) Special Categories such as health information	UK GDPR Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller.
Safeguarding a) Identity (b) Contact (c) Special Categories such as health information	Statutory duty under the Care Act 2014, Children Act 2004 and Children and Social Care Act 2017. UK GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. UK GDPR Article 9 (2) (b) Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or the

	data subject in the field of social protection law in so far as it is authorised by Union or Member State Law.
To investigate and respond to a complaint (including whistleblowing) (a) Identity (b) Contact (c) Special Categories	UK GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. UK GDPR Article 9 (2) (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes
Commissioning, Audit and Planning Purposes (a) Identity (b) Contact (c) Special Categories	Article 6 (1) (c) Processing is necessary for compliance with a legal obligation. Article 6 (1) (e) 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. Article 9 (2) (h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
Research (a) Identity (b) Contact (c) Special Categories	Article 6 (1) (e)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. Article 9 (2) (j) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).
Employment Purpose (staff and volunteers) (a) Identity (b) Contact (c) Special Categories	Article 6 (1) (e) 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. Article 9 (2) (b) Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or the data subject in the field of social protection law in so far as it is authorised by Union or Member State law. Personal data processed in relation to the Disclosure and Barring Service (DBS checks) falls under the UK GDPR (Article 10) and the provision of Safeguarding Vulnerable Groups Act 2006.
Surveys e.g. monitoring improvement of care	*The Trust may contract third party organisations to work on survey*

(a) Identity (b) Contact (c) Special Categories	*development and analysis on its behalf. In such circumstances, participants will be notified in advance of their data being gathered.* UK GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. UK GDPR Article 9 (2) (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
Processing of data relating to criminal conviction (c) Special Categories	The Trust ensures that the lawfulness of processing of special categories of personal data and criminal convictions data necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment under *UK GDPR Article 9 (2) (b)* is permitted under *DPA Section 10(1) (a):* **Additional conditions for processing data relating to criminal conviction data** • *DPA Schedule 1, Part 3* sets out the additional conditions which must be met when processing data relating to criminal conviction data. Therefore, in line with clause 29 of this Schedule, the Trust relies on the consent of the data subject/staff to process their personal data relating to criminal conviction data by virtue of employment.
Statutory Disclosure Trust may be legally required to share personal data concerning health with law enforcements and regulatory bodies such as: NHS England, the Police, Courts of Justice, HMRC, DVLA, Medico-Legal, NHS Counter Fraud, and the Health Service ombudsman	DPA 2018 Schedule 2, part 1, section 2 crime and taxation general In some circumstances for the purposes of: Safeguarding, investigation, prevention, or detection of crime. apprehension or prosecution of offenders. the assessment or collection of any tax or duty or, of any imposition of a similar nature.
Statutory Collection Sharing of personal data concerning health with NHS Digital for the purpose of National Data collections/ extraction	Article 9 (2) (h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of

	Union or Member State law or a contract with a health professional.

3. Summary of actions to implement policy

Publication on the Trust Internet and intranet.
Inclusion in Information Governance Training.

4. Legal and policy framework

- The Data Protection Act 2018
- UK General Data Protection Act 2020
- Freedom of Information Act 2000
- Human Rights Act 1998
- Trust Privacy notice and Employee Privacy Notice
- Data Protection Impact Assessment Template
- NHSx Records Management Code of Practice 2021
- Integrated Information Governance
- Records of Processing Activity

5. Key responsibilities

The Chief Executive has ultimate responsibility for ensuring that mechanisms are in place for the overall implementation, monitoring and revision of policy.
Senior Information Risk Officer (SIRO) will oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing Information Governance Framework.
The Caldicott Guardian is responsible at Board level for approving and ensuring that national and local policies on the handling of confidential personal information are implemented. The Caldicott Guardian also has the added responsibility for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
Head of Quality Governance, is responsible for ensuring that:

- In conjunction with the Policy Lead identifies resource implications to facilitate implementation and compliance.
- Training and monitoring systems are in place.
- Regular review of the policy takes place.

Service Directors are responsible for implementation of the policy within their own spheres of management and must ensure that:

- All new and existing staff have access to and are informed of the policy
- Ensure that local written procedures support and comply with the policy
- Ensure the policy is reviewed regularly
- Staff training needs are identified and met to enable implementation of the policy

The Head of Information Governance provides advice and highlights risks associated with Trust compliance with data protection legislation and Information Governance policies and guidance.

The Data Protection Officer (DPO) responsibilities include:

- Informing and advising organisations about complying with General Data Protection Regulation (UK GDPR) and other data protection legislations
- Monitoring compliance with UK GDPR and data protection laws with the support of Head of IG – including staff training and internal audits;
- Advising on and monitoring data protection impact assessments;
- Cooperating with the ICO.

All Trust staff are responsible for ensuring that they:
- Are familiar with the content of the relevant policy and follow its requirements
- Work within, and do not exceed, their own sphere of competence.

6. Training required to implement policy

Employees of the Trust will be required to attend Core Induction, including attendance at the mandatory Data Security and Protection (Information Governance) training session.

Data Security and Protection (Information Governance) training is mandatory for all employees, and must be done yearly. (Refer to the Trust mandatory training matrix).

7. Monitoring and evaluation

There should be clear criteria by which to monitor implementation of the policy and evaluate its effectiveness and appropriateness. This is usually expressed as a table.

Measure	Lead (Name and Title)	Group/ Committee that measures will be reported to by lead	Frequency of Reporting
Outlined in Table Below	Head of Information Governance	Information Management Group	Quarterly

Accountability principle

i. The Trust maintains records of processing activities under Article 30 of the UK GDPR
ii. The Trust has an Integrated Information Governance Policy
iii. The Trust carries out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?

Principle (a): lawfulness, fairness and transparency

i. The appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data is outlined in the Trust's privacy notice
ii. The Trust is open and honest when collecting SC/CO data.

Principle (b): purpose limitation

i. The Trust has clearly identified its purpose(s) for processing the SC/CO data.
ii. The Trust has included appropriate details of these purposes in its privacy notice(s) for individuals

iii. Any plan to use personal data for a new purpose (other than a legal obligation or function set out in law), the Trust will check that this is compatible with the original purpose.

Principle (c): data minimisation

i. The Trust is satisfied that we only collect SC/CO personal data we need for our specified purposes, and this is assessed during the Data Protection Impact Assessment (DPIA).
ii. The Trust periodically reviews data in accordance with the NHSx Records Management Code of Practice 2021 and takes appropriate action when necessary.

Principle (d): accuracy

i. The Trust has appropriate processes in place to check the accuracy of the SC/CO data collected.
ii. The Trust has implemented a Data Quality Strategy and regularly reviews the accuracy of data.

Principle (e): storage limitation

i. The Trust has an Integrated Information Governance Policy which consider how long we keep the SC/CO data and justify this amount of time. This is derived from the NHS Records Management Code of Practice (2021)

Principle (f): integrity and confidentiality (security)

i. The Trust assesses the appropriate level of security required for this data processing and this is part of the Data Protection Impact Assessment (DPIA).
ii. The Trust has an Integrated Information Governance Policy which outlines the steps to ensure SC/ CO is data is protected.
iii. The Trust has technical measures or controls in place because of the circumstances and the type of SC/CO data processed including an Information Asset Register.

Appendices

None

Oxford Health
NHS Foundation Trust

Equality Analysis (EqA) Screening Form

Name of Policy/Procedure/Practice/Project/Programme/Plan: Appropriate Policy Document

Equality Analysis (formerly known as Equality Impact Assessment) is a thorough and systematic analysis of a policy, practice or procedure to ensure it is not unlawfully discriminating against any group with a protected characteristic.

An equality analysis is:

- A tool for delivering equality
- A key way of demonstrating that you have given 'due regard' to equality considerations as prescribed by the public sector equality duties in the Equality Act 2010
- Part of good policy and service delivery governance
- A positive activity which should identify improvements

Please use this EqA Screening Form to examine and identify any differential impact for any of the protected characteristics and to prompt mitigation of the adverse/negative impact before it is approved by the relevant committee.

This Screening Form can be used at the beginning of the equality analysis process to gather initial feedback, thoughts and ideas, or at quarterly intervals to monitor implementation of a project/programme, or at the end on completion to assess impact or outcome.

If this Screening Form reveals any adverse/negative impact for any of the protected characteristics listed below, you may need to complete a full Equality Analysis (Form EqA1). For further details (including a copy of the EqA1 Form), please see Equality Analysis Procedure and Guidance which can be found on the Polices Site.

For advice, information and guidance, please contact the Head of Inclusion at: EqualityandInclusion@oxfordhealth.nhs.uk

Protected Characteristic	Positive Impact	Neutral Impact	Negative Impact	Comments/Evidence
	√	√	√	
Age	✓			
Disability	✓			
Sex/Gender	✓			
Race/Ethnicity	✓			
All Faiths & None	✓			
Sexual Orientation	✓			
Transgender	✓			
Pregnancy & Maternity	✓			
Marriage & Civil Partnership	✓			

Completed by:-
Name: Mark Underwood
Title: Head of Information Governance
Date: 21/04/2022