nuffieldtrust

Privacy Policy

Category	Data Protection
Version	0.1
Classification	Internal

Document Control

Organisation	Nuffield Trust
Title	Privacy Policy
Author	Tony Harbon
Filename	Privacy Policy.docx
Owner	DPO
Subject	Nuffield Trust Privacy Policy
Protective Marking	Internal
Review date	

Revision History

Revision Date	Version Number	Revised By	Description of Revision
17/10/18	0.1	Tony Harbon	
26/3/18	1.0	Tony Harbon	Editorial

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address / Location
All Employees		

Table of Contents

Contents

Approvals & Review

The policy applies and will be enforced as of 15th January 2019.
This Policy shall be reviewed by Nuffield Trust no later than 15th January 2019.

Version Control

The current official copy of this policy shall be located in the following folder:

X:\Staff Material\Information Governance\Trust-Wide\Policy

If this document was found in any other location, the reader should check the policy portal to confirm they are reading the current document. The version information is as follows:

Version	Description	Date	Author	Reviewer

Policy Owner

The Owner of this policy is the incumbent Data Protection Officer.

Purpose

An organisation which controls processing activities, involving Personal or Sensitive Data relating to European Union Data Subjects, must comply with the General Data Protection Regulation 2016 ('GDPR'), the Data Protection Act 2018 and the Privacy & Electronic Communications Regulation 2003 ('PECR'). This policy sets out the requirements all those in scope must adhere.

This Policy is subject to all the laws, rules and regulations that this organisation is governed by.
In the event this policy allows the exercise of discretion, such discretion must be exercised within the confines of the organisation's statutory obligations and must not contravene any of its legal, accounting or other regulatory requirements.

Risk Appetite Statement

The Nuffield Trust's Risk Appetite for a material breach of GDPR compliance is LOW.
The Trust has identified the key data protection risks as; personal data breaches, failing to uphold Data Subjects' rights and reputational damage.

Scope

The scope of this policy covers all Processing activities and supporting Information Systems involving Personal or Sensitive Data where the organisation acts as the Controller. This includes all personal data in electronic or physical form that is stored in a filing system.

The scope of this policy covers all global geographic territories. For the avoidance of doubt, this includes Third Countries outside the European Union (EU).

The scope of this policy covers all Employees, Contractors, and Third Parties, Processors or others who process Personal Data on behalf of the organisation.

Requirements

Principles
All Processing activities shall be:

- Collected for specified, explicit and legitimate purposes only
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed lawfully, fairly and in a transparent manner
- Processed securely, in an appropriate manner to maintain security
- Adequate, relevant and limited to what is necessary

Data Protection Officer

- A Data Protection Officer has been appointed.
- The Data Protection Officer shall support the organisation in upholding the rights of Data Subjects as it relates to the organisation's processing activities.
- The Data Protection Officer shall respond to enquiries from Data Subjects in a timely manner.
- The Data Protection Officer shall establish and maintain a programme to monitor compliance with this policy.
- The Data Protection Officer shall establish and maintain a General Data Protection training and awareness programme.
- The Data Protection Officer shall support compliance with this policy by providing support and advice as it relates to complying with the requirements of this policy.
- The Data Protection Officer shall be provided timely and appropriate access to information and information systems as it relates to the discharge of their duties.
- Details of the Data Protection Officer, and their contact details shall be made publically available.

The Data Protection Officer shall maintain the following registers:

- Register of Processing Activities
- Register of Data Protection Impact Assessments (DPIAs)
- Register for Data Protection Metrics
- Register for Data Subject Enquiries

The Data Protection Officer shall report notifiable personal data breaches to the Supervisory Authority no later than 72 hours after the breach has been detected.

Accountability

- A record of processing activities shall be provided to the Data Protection Officer
- A System Owner shall be appointed for all Information Systems containing Personal or Sensitive Data. The System Owner shall not be from IT unless IT is performing the primary processing activity (e.g. IT operate the Service Desk System and so an IT Manager could be assigned as System Owner).
- System Ownership shall not be assigned to a person who does not have budgetary responsibility for the Information System.
- System Ownership shall not be assigned to a person who does not hold formal authority over those carrying out processing activity within the Information System.
- A System Owner may delegate responsibility for operational tasks relating to this policy but shall not delegate accountability.
- A System Owner may seek advice in the discharge of their duties but remains accountable for any subsequent decisions taken (e.g. acceptance of risk).
- Processing activities shall be documented and a Process Owner appointed
- Process Ownership shall not be assigned to a person who does not hold formal authority over those carrying out processing activity within the Information System.

Lawfulness of Processing

Process Owners shall ensure processing is lawful and document the lawful grounds for processing. With the exception of storage, processing shall cease immediately where there are no longer lawful grounds for processing.

Transparency

- Process Owners shall ensure information related to their processing activities is made available to the Data Protection Officer so that an organisational Data Protection notice may be published.
- Data Subjects shall be informed of processing activities and provided statutory information at the time data is collected.
- Where data is collected from a source other than the Data Subject, they shall be informed of processing activities and provided statutory information as soon as practicable but no less than 10 working days.

- Process Owners shall review the published Data Protection notice quarterly for any omissions or inaccuracies relating to their processes. The Process Owner shall report inaccuracies to the Data Protection Officer within 5 working days.

Data Protection by Design & Default

Information Systems and Processes shall be designed to comply with the requirements of this policy. Process and System Owners shall implement appropriate technical and organisational measures to ensure that data protection is incorporated into processes and systems, by design and default.

Processing activities and supporting Information Systems shall be designed to ensure the minimum personal data is stored and for the minimum period necessary.

All Information Systems shall ensure their systems undergo a Data Protection Impact Assessment (DPIA) which contains at a minimum:

A systematic description of the envisaged processing operations and the purposes of the processing. An assessment of the necessity and proportionality of the processing operations in relation to the purposes:

- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this policy taking into account the rights and legitimate interests of data subjects and other persons concerned
- The System Owner shall consult with the Data Protection Officer in relation to the completion of the DPIA.
- The Data Protection Officer shall, where the risk to Data Subjects' rights is deemed HIGH, consult with the Supervisory Authority.
- System Owners shall ensure systems are explicitly designed to minimise the impact involved in upholding Data Subjects' rights.
- Process Owners shall ensure processes are explicitly designed to minimise the impact involved in upholding Data Subjects' rights.

Security of Processing

System Owners shall be accountable for ensuring systems meet the minimum required standards for security, including, but not limited to:

- Identity & Access Management
- Patch & Vulnerability Management

- Change Management
- Backup & Restoration
- IT Service Continuity Planning and Testing
- Development and Testing Activities
- Security breach monitoring and detection
- Information Systems, containing personal or sensitive data, exposed to the Internet or a Third Party, shall be subject to an independent, risk-based penetration test to an agreed scope, no less than annually.
- System Owners shall ensure all issues identified are appropriate treated commensurate with the Board's risk appetite.
- Personal Data Breaches shall be reported to the Data Protection Officer as soon as possible but no later than 1 working day after detection.

Accuracy of Processing

- Process Owners shall ensure data remains accurate and where inaccurate corrected as soon as possible but no later than 5 working days from when the error is reported and verified.
- Process Owners of processes involving automated decision making or profiling shall document an alternative manual process and ensure appropriate resources are trained to carry out the manual process if required.
- A Data Subject shall have a right not to be subject to an automated decision or profiling. Process Owner shall ensure this right is respected except where statutory exemptions apply.

Retention

With the exception of data held under statutory exemptions, personal data shall not be retained any longer than necessary.

Pseudonymisation

Administrative data (that is, data recorded in the course of delivering front-line care) has huge potential for aiding the study of health systems, particularly when analysed at individual patient level. These data become even more powerful when linked across multiple databases to provide a history of an individual’s service use over time which enable us to understand the consequences or outcome of health care services. Research using these data has produced many benefits for patients, such as receiving more effective treatments and better services.

As with any patient level records there have to be safeguards to protect potentially sensitive information. These data have to be used in an environment that adheres to certain regulations and guidance help to protect privacy and confidentiality. So for example one approach is to remove those information items that identify individuals - like names, addresses and dates of birth.
The Nuffield Trust uses de-identified patient level data in several of our projects to research the way health services are used and how they can be developed to better meet the needs of their users.

Receiving pseudonymised data
The vast majority of data received and held by Nuffield Trust are already pseudonymised by the organisation sending them to us. Where these are received from HSCIC or other Accredited Safe Havens we can be confident that the pseudonymisation is robust and conforms to best practice. Where we are receiving locally pseudonymised data we will advise them on the pseudonymisation process. This includes recommending appropriate pseudonymisation software (for example OpenPseudonymiser) and that the pseudonymisation conforms to best practice (currently Secure Hash 256 with passkey appended to NHS number before pseudonymisation).
All transfers of de-identified patient level data happen via our SFTP software and follow the processes set out in the Sensitive Data Security Policy.

Distributing pseudonymised data
The Nuffield Trust does not distribute patient-level data to any other organisation.

Data Subject Access

- Process Owners shall ensure those processing data understand how to identify a Data Subject Access Request.

- Data Subject Access Requests shall be recorded in a register owned by the Data Protection Officer.

- Data Subject Access Requests shall be completed as soon as possible but no more than 30 calendar days.

- Data Subject Access Requests shall not incur a charge unless the request is repeated or excessive.

- Data Subject Access Request shall be processed electronically if this is requested by the Data Subject.

- Reasonable steps shall be taken to verify the identity of the Data Subject prior to providing access to their personal data.

- System Owners shall ensure appropriate resource is made available to support Data Subject access requests.

- Reasonable steps shall be made to seek the permission of third parties prior to including their information within an access request. Where permission is not provided, the Data Protection Officer shall determine whether data should be provided or redacted.

- Requested information shall be communicated to the Data Subject securely.

Third Party Processing

- Processing activities shall not be outsourced to a third party without a binding written contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of Data Subjects and the obligations and rights of this Organisation.

- Process Owners shall use only third-party Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this policy and ensure the protection of the rights of the Data Subject.

- Process and System Owners shall consult with, and obtain a written recommendation from the Data Protection Officer and representatives from Legal, Procurement, Information Security, Business Continuity and Risk prior to signing a contract with a third party Processor and with sufficient time (at least 5 days) to carry out effective due-diligence on the proposed outsourced process and the third party Processors data protection technical and organisational controls.

- Where recognised data security certification is not present, Process and System Owners may choose to engage an independent (internal or external) assessor that is professionally qualified to assess the third party Processor's data protection technical and organisations controls.

- Process and System Owners engaging third-party Processors shall ensure continuing compliance with this policy and maintain accurate records of relevant meetings and compliance visits including supporting evidence of the third party Processor's ongoing compliance.

Roles & Responsibilities

- The Board has overall responsibility for this policy, and for reviewing the effectiveness of actions taken in response to concerns raised in this policy.

- The Senior Management Team shall ensure appropriate resources are made available to support the implementation of this policy throughout all in-scope areas.

- All those in scope of this policy are responsible for adhering to the requirements of this policy

- The Data Protection Officer is responsible for monitoring compliance with this policy and shall provide periodic reporting to Nuffield Trust Board and Nuffield Trust Senior Management Team on the organisation's compliance with this policy.

- The Data Protection Officer shall be the contact point for all matters relating to the Supervisory Authority (SA)

- The IT Manager is responsible for providing information security support as it relates to this policy.

- Those described as Owners of this policy are responsible for ensuring their Processes, and Information Systems meet the minimum requirements of all in-scope policies.

- The Owners of the policies, detailed herein shall ensure requirements are amended to reflect the requirements of this policy.

- The HR Manager shall ensure Human Resources processing is compliant with the requirements of this policy.

- The Director of Communications shall ensure processing related to Communications activities is compliant with the requirements of this policy.

- The Director of Policy shall ensure processing related to Policy activities is compliant with the requirements of this policy.

- The Director of Research shall ensure processing related to Research activities is compliant with the requirements of this policy.

- The Deputy Director of Operations shall ensure procurement and administration processes are compliant with the requirements of this policy.

- The Data Protection Officer shall provide the Board with independent assurance that the organisation is adhering to the requirements of this policy.

Related Policies

This policy should not be read in isolation. The following policies also include specific and supporting requirements:

- Data Classification Policy
- Information Handling Policy
- Exercise of Rights Policy
- Information Security Policy
- Incident Response Policy

Links to supporting Templates

Templates and other supporting materials can be found in the following folder on the Staff Materials Drive:

X:\Staff Material\Information Governance\Trust-Wide\Policy

Glossary of Terms

The following definitions are crucial to understanding the General Data Protection Regulation. When dealing with personal data, you must keep the following definitions in mind as they will be vital to understanding your data protection roles and responsibilities. This list is not exhaustive and more terms will be described throughout the book but initially, the most useful are as follows:

Natural Person: Essentially an EU citizen who is alive.

A Natural Person: may also be referred to as a Data Subject.

Child: For the purposes of GDPR is a Natural person who requires parental consent, usually if they are below 16. The EU Member States can, however, reduce the requirement for consent to those no younger than 13 (i.e. if the Natural Person is over 13 parental consent would not be required). The UK has adopted 13 as the age at which parental consent is not required.

Personal Data: any information relating to an identified or identifiable Natural Person (or 'Data Subject'); an identifiable Natural Person is one 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 Data: special categories of information relating to an identified or identifiable Natural Person (or 'Data Subject'). Examples include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, sex life or sexual orientation.

Processing: any 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a Natural Person, in particular to analyse or predict aspects concerning that Natural Person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Consent: any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.

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

EU Member State: any country party to the founding treaties of the European Union (EU) and thereby subject to the privileges and obligations of membership. Member States are subject to binding laws in exchange for representation within the common legislative and judicial institutions.

Third Country: any country which is not an EU Member State (e.g. USA, India, China or the Philippines)

Supervisory Authority: the regulator within a European country who will provide regulatory oversight for GDPR, provide guidance and advice and, where necessary impose corrective actions or administrative fines.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Protection Impact Assessment (DPIA): An assessment of the impact of the envisaged processing operations on the protection of personal data and the rights and freedoms of natural persons.

Subject Access Request (SAR): A request, made by a natural person, to access personal data held by a Controller or Processor,

Data Protection Officer (Data Protection Officer): a person with expert knowledge of data protection law and practices who assists the Controller or Processor to monitor internal compliance with GDPR. Such data protection officers, whether or not they are an employee of the Controller, should be in a position to perform their duties and tasks in an independent manner.

The Lawful Basis for Processing

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

- Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.

- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

What are the Lawful Bases for Processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

- **Vital interests:** the processing is necessary to protect someone's life.

- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)