# Trust wide Privacy Notice

## Introduction

Norfolk and Suffolk NHS Foundation Trust (the Trust) provides mental health care services to the residents of Norfolk and Suffolk. Our services include mental health, learning disabilities, eating disorders and wellbeing. The Trust is registered with the Information Commissioners Officer (ICO) as a Data Controller.

With effect from the 25th May 2018, the EU General Data Protection Regulations (GDPR) as enacted by the Data Protection Act 2018 (DPA 18) comes into force. GDPR and the DPA18 covers personal data held manually and electronically by organisations within the United Kingdom.

Within this Privacy Notice, the principles adopted by the Trust to meet its legal obligations under GDPR, DPA 18 and the NHS requirements concerning confidentiality and information security standards have been set out.

The Trust collects and processes personal data in the course of its business activities. The personal data we hold relates to current, past and prospective service users, carers, staff past and present, volunteers, governors, members, commissioners, suppliers, contractors, customers, and other stakeholders.

The Trust has a legal obligation to comply with all appropriate legislation in respect of personal data, information and ICT security. This includes the collection and processing of certain types of personal data to comply with the legal requirements of government departments. The Trust also has a duty to comply with guidance issued by the Department of Health (DoH), The NHS Executive and other advisory groups to the NHS and guidance issued by professional bodies.

## Compliance with GDPR

The Trust regards the confidence and trust of its service users, staff and stakeholders as a crucial element in its role in delivering the highest quality health care services. The lawful and correct processing of personal data is a key part of building and maintaining that trust and confidence. The Trust will fully discharge its responsibilities implied by the Principles contained within the GDPR (Article 5) by putting in place the following procedures, which will be monitored through annual audits:

- Comply with the ICO's guide "Good Practice Guidance on Privacy by Design" (Article 25 GDPR)
- Fully implement all aspects of the GDPR and publish information so that all service users, staff and stakeholders are aware of their rights under GDPR
- Ensure all staff understand the GDPR, by holding mandatory training for all staff
- Implement adequate and appropriate physical and technical security measures and organisational measures to ensure the security of all personal data held by the Trust, or by other organisations on behalf of the Trust
- Meet its legal obligations to specify the purposes for which personal data is used by a series of Privacy Notices
- Only collect and process appropriate personal data to the extent that it is needed to fulfil operational needs or to comply with any legal requirement and fully observe conditions regarding the fair collection and use of personal data
- Ensure the quality and accuracy of the personal data used
- To keep personal data securely and in line with the DoH Records Management Code of Practice for Health and Social Care 2016
- Ensure that the rights of people about whom personal data is held can be exercised fully under the legislation
- Ensure that the necessary measures to ensure the proper disclosure of personal data between agencies are taken
-

- Where there is a requirement to send personal data outside the European Economic Area (EEA), staff will obtain prior authorisation from IG Services to ensure that the necessary safeguards and measures are implemented prior to the disclosure of personal data
- Ensure full compliance with the new notification process under GDPR to the ICO

## Roles & Responsibilities

The Chief Executive has overall responsibility for the implementation and delivery of the GDPR on behalf of the Trust.

A requirement of the GDPR (Articles 37-39) is the appointment of a Data Protection Officer (DPO) who has devolved responsibility from the Chief Executive in relation to GDPR.

All NHS Foundation Trusts also have a Caldicott Guardian who is a senior person responsible for protecting the confidentiality of service users and enabling appropriate information sharing.

Detailed below are the key roles and responsibilities of these roles:

### Data Protection Officer

- Facilitating the implementation of GDPR
- Supporting Trust staff to understand their responsibilities
- Jointly responsible (with the Caldicott Guardian) for ensuring the effective integration of respective policies relating to personal data held within health records

### Caldicott Guardian

- Advising Trust staff
- Ensuring adequate arrangements are implemented to protect personal data held within health records
- Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of personal data
- A strategic role, which involves representing and championing issues related to information sharing at Board or management team level

### Staff

All staff within the Trust should ensure that personal data is processed in accordance with the GDPR and the rights of the individual. Any concerns relating to confidentiality should be dealt with professionally and where appropriate referred to the Data Protection Officer.

## Our Lawful Reasons for using your personal data

The below lawful reasons have been identified under GDPR these enable the Trust to process personal data without the requirement to seek consent from the data subject.

### Direct Care

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 a patient for their direct care.

| | |
|---|---|
| 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. |
| 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. |

### Safeguarding

The Children's Act 1989 (CA) establishes implied powers for local authorities to share personal data to safeguard children. The CA also allows local authorities to request help from Foundation Trusts to safeguard and promote the welfare of children within their area who are in need.

The CA sets out a clear legal framework for how local authorities and other parts of the system should protect adults at risk of abuse or neglect. Local authorities have a duty to make enquiries where an adult is experiencing or is at risk of experiencing abuse or neglect, and has a duty to collaborate with partners generally and in specific cases.

| | |
|---|---|
| 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. |
| 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. |

### Commissioning and Planning Purposes

Most national and local flows of personal data in support of commissioning are established by NHS Digital either centrally, or for local flows by its Data Services for Commissioners Regional Offices (DSCRO).

These flows do not operate on the basis of consent for confidentiality or data protection purposes. Where the collection or provision of personal data is a legal requirement, GDPR still needs to be complied with.

The appropriate lawful reasons for providers of the personal data is 6 (1) (e) and 9 (2) (h) under Section 251B of the Health and Social Care Act 2012. When the processing is not supported under Section 251B of the Health and Social Care Act 2012 the lawful reasons are 6 (1) (c) and 9 (2) (h).

| | |
|---|---|
| 6 (1) (c) | Processing is necessary for compliance with a legal obligation. |
| 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. |
| 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

For research purposes, the common law duty of confidentiality must still be met through consent. This requirement has not changed under the GDPR. Consent is still needed for people outside the care team to access and use service user personal data for research, unless you have Section 251B of the Health and Social Care Act 2012 support.

| | |
|---|---|
| 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. |
| 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). |

### Regulatory and Public Health Functions

For performing regulatory and public health functions the below lawful reasons are both required. This function would also include processing contracts that the Trust has entered into.

| | |
|---|---|
| 6 (1) (c) | Processing is necessary for compliance with a legal obligation. |
| 9 (2) (i) | Processing is 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. |

### Employment Purposes (staff and volunteers)

For employment purposes the below lawful reasons for lawful processing will apply this includes special categories of data such as health data for employment purposes.

| | |
|---|---|
| 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. |
| 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 GDPR (Article 10) and the provision of Safeguarding Vulnerable Groups Act 2006.

### Foundation Trust Governors and Members

NHS Act 2006 sets out the legal requirements of a NHS Foundation Trust.

| | |
|---|---|
| 6 (1) (c) | Processing is necessary for compliance with a legal obligation to which the controller is subject |
| 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. |
| 9 (2) (g) | Processing is necessary for reasons of substantial public interest. |

## Categories and Sources of Personal Data

This privacy notice covers all aspects of processing of personal data carried out by the Trust during its normal business activities the below list is not exhaustive:

### Trust business activities

- Mental and physical healthcare
- Access and assessment teams
- Primary care teams
- Learning disability services
- Child and adult protection
- Human resources (including DBS checks)
- Payroll and finance
- Procurement
- Estates and facilities (maintenance)
- Occupational health
- Foundation Trust membership
- Volunteers

### Personal data we may process

- Personal details
- Family details
- Education, training
- Employment details
- Financial details
- Goods and services
- Lifestyle and social circumstances
- Visual images, personal appearance and behaviour
- Details held on patients' records
- Responses to surveys

**Sensitive personal data we may process**

- Racial and ethnic origin
- Offences and alleged offences
- Criminal proceedings, outcomes and sentences
- Trade union membership
- Physical or mental health details
- Religious or similar beliefs
- Sexual life

**We process data about**

- Service users
- Suppliers
- Employees
- Volunteers
- Governors
- Members
- Complaints
- Survey respondents
- Professional experts and consultants
- Individuals captured by CCTV images

**Sources of data we process**

- Other healthcare providers
- Social care providers
- Local and national health and social care organisations
- Contractors
- Suppliers
- Professional bodies
- Data subject (service users and employees)

**How we store data**

- Manually stored paper data e.g. card index files, medical records
- Computer references paper data e.g. health records
- Personnel records etc
- Computerised data held in computer applications and databases
- Tapes and other data from CCTV systems
- Data held offsite in archive storage
- Data held on CD ROMS, computer disks, memory sticks etc.
- Data is retained in line with the DoH Records Management Code of Practice for Health and Social Care 2016

## Requests to share personal data

The Trust receives requests to share personal data from other agencies and sources these are actioned by the Information Rights team. Personal data will be shared with the following organisations without the data subjects consent if a lawful reason to share the personal data under GDPR is identified:

- Health and social care providers
- Local authorities
- Commissioners
- Safeguarding agencies

- Police forces and authorities with investigative powers
- Organisations with a defined lawful reason (e.g. Department of Work and Pensions)

When sharing personal data with third parties that are not health and social care providers, such as relatives the common law duty of confidentiality must still be met through consent. Where a child is under the age of 13 then consent (under the common law duty of confidentiality) of those with parental responsibility will be sought. These types of requests would include requests from organisations or solicitors who have been given authority in writing to act on behalf of the data subject.

## Data Subject Rights

Individuals still have rights under the GDPR just like they did under the Data Protection Act 1998. The Trust will ensure that all individuals are aware of their rights under the legislation and will comply with the delivery of these rights to individuals.

### Right to be Informed (Articles 12-14 GDPR)

Details relating to the personal data processed by the Trust is detailed within this privacy notice. A copy of this privacy notice is available to view or download from the Trust website www.nsft.nhs.uk or a hard copy may be requested from the Information Rights Team.

### Right to Access (Subject Access Requests) Article 15 GDPR

- All data subjects, or someone acting on their behalf, can request a copy of their personal data held by the Trust
- All requests for copies of personal data must be made in writing to the Information Rights Team who will validate and action the request
- If third party data is included in the personal data being requested this will be redacted unless we have the consent from the third party to release their personal data
- The Trust may on occasion be unable to provide access to personal data held if the release is likely to be detrimental to health or cause harm. These circumstances would be reviewed on a case-by-case basis
- The Trust must provide a copy of the personal data free of charge. However, the Trust can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The Trust may also charge a reasonable fee to comply with requests for further copies of the same personal data. The fee will be based on the administrative cost of providing the personal data
- The Trust has one calendar month to provide the personal data requested. If the personal data being requested is complex or numerous then the Trust is able to extend the period of compliance by a further two months. The Trust will notify the requestor of the extension to the timeframe and explain why this is necessary within one calendar month of receipt of the initial request

### Right to Rectification (Article 16 GDPR)

- All data subjects can ask the Trust to review any of the information that they feel is inaccurate
- Please note that the rectification of health records is dealt with on a case by case basis however the Trust follows the Department of Health Guidelines as summarised below:
  - Credible records are an important aid in providing safe healthcare
  - Records should reflect the observations, judgements and factual data collected by the contributing health professional
  - An opinion or judgement recorded by a health professional, whether accurate or not, should not be deleted
  - Retaining relevant records is essential for understanding the decisions that were made and to audit the quality of care
  - If a service user feels that personal data recorded on their health record is incorrect, they should first make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended

  - Where both parties agree that the records are factually inaccurate it should be amended to clearly display the correction whilst ensuring that the original record is still legible. An explanation for the correction should also be added to the records
  - An amended version of the records should be shared with anyone who received the inaccurate records
  - Where the health professional and patient disagree about the accuracy of the entry, the Department of Health recommends that the data controller should allow the service user to include a statement within their record to the effect that they disagree with the content
- If the data subject is still unhappy then they should contact the Data Protection Officer in writing who will investigate the request for rectification of personal data within a health record on a case-by-case basis
- Requests to rectify other personal data held by the Trust should be made in writing to the Data Protection Officer who will oversee the request for rectification on a case-by-case basis

**Right to Erasure (Article 17 GDPR)**

- The Trust processes the majority of personal data under the lawful reason of 6 (1) (e) public interest and 9 (2) (h) in the interest of public health. Therefore, the right to erasure does not apply to personal data processed under these lawful reasons
- If a data subject still believes that they have a right to request erasure then this request should be made in writing to the Data Protection Officer to review on a case-by-case basis

**Right to Restriction of Processing (Article 18 GDPR)**

All data subjects have the right to require the Trust to restrict processing where:

- Accuracy is contested by the data subject
- Processing is unlawful, and the subject opposes erasure
- The data controller no longer needs the data, but the subject requires it to be kept for legal claims
- The data subject has objected, pending verification of legitimate grounds

Requests to restrict processing should be made in writing to the Data Protection Officer to review on a case-by-case basis.

**Right to Object (Article 21 GDPR)**

- The right to object does not apply where the Trust can demonstrate compelling legitimate grounds for the processing
- Requests to object to processing should be made in writing to the Data Protection Officer, to review on a case-by-case basis

**Automated Decision-making including profiling (Article 22 GDPR)**

The Trust does not process any personal data using automated decision-making processes or profiling, therefore the rights in relation to this will not apply to personal data held by the Trust.

**Right to Data Portability (Article 20 GDPR)**

The right to data portability is only available where processing is based on consent and the processing is automated. The Trusts lawful reasons are not based on consent and the Trust does not process personal data using automated decision-making processes.

**Right to Complain**

- A data subject can complain directly to the Trust if they are concerned about how the Trust is processing their personal data. In the first instance, a complaint should be made in writing to the Data Protection Officer
- Alternatively, a data subject has a right to complain directly to the ICO who oversees how organisations within the United Kingdom manage personal data

## For further information contact

Information Rights Team
Norfolk and Suffolk NHS Foundation Trust
Kestrel House
Hellesdon Hospital
Drayton High Road
Norwich
NR6 5BE

Tel: 01603 421108 / 421264
Email: informationrights@nsft.nhs.uk

Mr Richard Green
Data Protection Officer
Norfolk and Suffolk NHS Foundation Trust
Hellesdon Hospital
Drayton High Road
Norwich
NR6 5BE

Tel: 01603 421578
Email: dataprotectionofficer@nsft.nhs.uk

Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545740
www.ico.gov.uk

## Supporting Information

### Definitions (From the General Data Protection Regulations) Article 4

**Personal Data** means any information relating to an identified or identifiable natural person **(**'**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 physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Controller** means 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; whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restrictions, erasure and destruction.

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

**Processing** means 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, organisations, structuring, storage, adaption or alteration, retrieval, consultation, use , disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients, the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

## The Principles of GDPR

Principles relating to the processing of data. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)
- Collected for specified, explicitly and legitimate purposes and not further processed in a manner that is incompatible with those purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (purpose limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
- Accurate and where necessary kept up to date, every reasonable step taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay (accuracy)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical; and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (storage limitations)
- Processed in a manner than ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality)
- The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 (accountability)

### Legislation to restrict disclosure of personal data

- Human Fertilisation and Embryology (disclosures of information) Act 1992
- Venereal Diseases 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1976

### Legislation requiring disclosure of personal data

- Public Health (Control of Diseases) Act 1984 and Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to the NHS Trusts from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984