

Policy Checklist

Policy name:	UK General Data Protection Regulations and Data Protection Act 2018 Policy
Lead Policy Author & Job Title:	[REDACTED] Head of Information Governance
Director responsible for Policy:	[REDACTED]
Directorate responsible for Policy:	Planning Performance & Informatics
Equality Screened by:	[REDACTED] Head of Information Governance
Trade Union consultation?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Policy Implementation Plan included?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Date approved by Policy Scrutiny Committee:	01 st September 2022
Date approved by SLT:	Click here to enter a date.
Policy circulated to:	Eg Directors, Assistant Directors, Heads of Service for onward distribution to line managers, Global email, Staff Newsletter
Policy uploaded to:	Eg SharePoint, Trust website

Version Control

Version:	4.2		
Supersedes:	Version 4.1		
Version History			
Version	Notes on revisions/modifications and who document was circulated or presented to	Date	Lead Author Policy
4.0	SHSCT Data Protection Act 2018 Policy V4.0	2019	Catherine Weaver
4.1	Revision to include reference to the UK leaving the EU (Para 1.3)	1 st September 2022	Catherine Weaver
4.2	Inclusion of 'appropriate policy document' requirements as Appendix 1.	1 st January 2024	Catherine Weaver

Contents

1.	INTRODUCTION.....	4
2.	PURPOSE.....	5
3.	SCOPE.....	5
4.	DATA PROTECTION PRINCIPLES.....	5
5.	DEFINITIONS.....	6
6.	PERSONAL DATA PROCESSED BY THE TRUST.....	7
7.	POLICY STATEMENT.....	9
8.	ROLES AND RESPONSIBILITIES.....	10
9.	LEGISLATIVE COMPLIANCE, RELEVANT POLICIES, PROCEDURES AND.....	12
	GUIDANCE.....	12
10.	EQUALITY AND HUMAN RIGHTS CONSIDERATION.....	13
11.	REVIEW OF POLICY.....	14
12.	SOURCES OF ADVICE AND FURTHER INFORMATION.....	14
	APPENDIX 1.....	15

SOUTHERN HEALTH & SOCIAL CARE TRUST

General UK Data Protection Regulation and Data Protection Act 2018 Policy

1. Introduction

- 1.1 The EU General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, has introduced a new framework of rights and duties for the protection of personal data. The Regulation harmonises data privacy laws across Europe and strengthens and extends individual's rights and protections in relation to their personal data.
- 1.2 The Data Protection Act 2018 (DPA) ensures the standards set out in the EU GDPR have effect in the UK. As well as strengthening some of the requirements of the EU GDPR the DPA also provides some exemptions from the EU GDPR.
- 1.3 When the UK left the European Union on the 31st January 2020 the EU GDPR transferred into UK law and became the UK GDPR.
- 1.4 The Southern Health & Social Care Trust is committed to ensuring that all of our employees, including volunteers, temporary staff, agency, bank staff, locums, and contractors comply with data protection legislation in order to safeguard the integrity and confidentiality of personal data processed by the Trust.
- 1.5 The priority of the Southern Health & Social Care Trust will be to ensure the rights and freedoms of individuals are protected before any processing of personal data. Employees are reminded that failure to comply with data protection legislation not only infringes on individuals rights, but may also result in the loss of reputation, loss of public trust, substantial fines and criminal proceedings against the Trust and / or individuals.

2. Purpose

- 2.1 The purpose of this policy is to set out our obligations under data protection laws, demonstrate our commitment to compliance with these, and explain the measures we have put in place in order to achieve this.
- 2.2 This Policy aims to fulfil the requirement for the fair, lawful and transparent processing of all personal data created or received by the Southern Health & Social Care Trust.
- 2.3 This Policy incorporates the requirements of the Appropriate Policy Document as required by the Data Protection Act 2018 (DPA). Further information on the categories of special category and criminal offence data processed under Schedule 1 of the DPA are referenced in appendix 1.

3. Scope

- 3.1 The Policy relates to all Trust staff including volunteers, temporary staff, agency, bank staff, and locums and also those staff contracted to carry outwork on behalf of the Trust.
- 3.2 The Policy relates to all records regardless of format or medium, including paper, electronic, audio, visual and photographic.

4. Data Protection Principles

- 4.1 Article 5 of the UK GDPR sets out six principles relating to the processing of personal data which the Trust must be able to demonstrate compliance with. Personal data shall be:
 - a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency'); We provide clear and transparent information to individuals about why we process their personal data, including our lawful basis, in our Privacy Notices. This includes information about why we process Special Category and Criminal Offence data

- b) collected for specified, explicit 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 not be considered to be incompatible with the initial purposes ('purpose limitation');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- e) 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 or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- f) processed in a manner that 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')."

5. Definitions

- 5.1 Personal data is information that relates to an identified or identifiable living individual
- 5.2 The UKGDPR definition of what constitutes personal data is more detailed and has been expanded to include a wide range of identifiers, reflecting changes in technology, and the way organisations collect information about people. For example, online identifiers like IP addresses can be personal data.

“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 the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”¹

5.3 Special categories (previously referred to as sensitive) personal data requires additional protection and is further defined in the Regulation to mean;

‘Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, or biometrics for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation...’²

5.4 Processing refers to any use of personal data including collection, storage, retrieval and destruction.

6. Personal Data Processed by the Trust

6.1 The Trust processes personal data in order to, but not limited to:

- Provide health and social care to patients and service users
- Help review the care given and ensure it is of the highest standard, this is done through internal audits and external inspections
- Training and educating staff
- Looking after the health and social welfare of the general public
- Investigating complaints or legal claims
- Preparing statistics on the Trust’s activity and performance
- Payment of Salaries, Travel, Subsistence, Sick Pay, Maternity Pay, Pension Administration etc.
- Her Majesty’s Revenue and Customs (HMRC)

¹UK GDPR Article 4 (1)

² UK GDPR Article 9 (1)

- Staff Engagement
- Management of Sickness Absences, Maternity Leave etc.
- Compliance with legal obligations, for example police investigations

6.2 The Trust processes different categories of personal data including, but not limited to:

- Name
- Address
- Date of Birth
- Contact Details
- Bank Details
- Employment Details
- Education and Training Details
- Personal identifiers e.g. identification numbers, online identifiers

6.3 The Trust processes the following special categories of personal data:

- Physical and / or Mental Health
- Racial or Ethnic Origin
- Political Opinions
- Religious Beliefs
- Sexual Life
- Trade Union Membership

6.4 The Trust may also process personal information about criminal offences such as:

- Criminal allegations
- Proceedings
- Convictions

Further information on the lawful basis and purposes of processing information in relation to special category and criminal offence data is available in appendix 1.

7. Policy Statement

7.1 In order to fulfil our obligations under data protection law the Trust is committed to:

- Making data subjects aware of when we collect personal data about them, and explaining the ways in which the information will be used;
- Making data subjects aware of their rights and how they can exercise them;
- Ensuring there is lawful basis for any processing;
- Ensuring that processing is fair
- Processing personal data which is adequate, relevant and limited to what is necessary for the intended purposes
- Ensuring the personal data is accurate and kept up to date
- Retaining personal data only for as long is needed in line with DoH Good Management, Good Records Retention and Disposal Schedule
- Taking appropriate technical and organisational measures to safeguard the integrity and confidentiality of personal data
- Ensuring that personal data is not transferred outside the EEA without appropriate safeguards
- Maintaining records of processing activities and organisational compliance

7.2 This is achieved through:

- Use of privacy notices and privacy information to inform data subjects wherever the collection and processing of personal data takes place, outlining the purposes for which the data will be used, who it will be shared with, how it will be securely retained, and how individuals may access it
- Efficient handling of subject access requests and other information rights requests
- Identification of a Data Protection Officer with specific operational responsibility for data protection in the Trust
- Training all Trust staff in data protection and information management in order to ensure they understand their obligations

- Operation and regular review of comprehensive procedures for the management and security of Trust information, regardless of media or format
- Maintenance of an information asset register and records of processing activities
- Regular monitoring, review and audit of the way in which personal data is collected, stored and used by the Trust
- Active use the DHSSPS Good Management, Good Records retention and disposal schedule to ensure information is only retained for as long as is necessary
- Ensuring individuals are aware of their obligations when being given access to personal data for research purposes
- Sharing information lawfully and in accordance with the Information Commissioner's Office Data Sharing Code of Practice
- Entering into a data access agreement whenever the Trust processes personal data for secondary purposes
- Entering into a contract when processing personal data on behalf of another data controller or where the Trust contracts data processing services
- Carrying out data protection impact assessments before we begin any processing of personal data which is likely to result in a high risk to individuals
- Carrying out information governance compliance checks to assess compliance with data protection laws
- Engaging and consulting with the Information Commissioner's Office
- Notifying the Information Commissioner's Office of any reportable personal data breaches within 72 hours of becoming aware and notifying individuals where there is a high risk to their rights and freedoms.

8. Roles and Responsibilities

- 8.1 The Trust's Chief Executive as "Accountable Officer" has overall responsibility for ensuring the aims of this policy are met.
- 8.2 The Personal Data Guardian is responsible for ensuring that the Trust is compliant with the confidentiality requirements of the UK GDPR and DPA

2018. The Trust Personal Data Guardian is the Medical Director.

8.2 The Director of Performance of Reform, as the Senior Information Risk Owner (SIRO), will take ownership of the organisation's information risk, act as an advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk.

8.3 The Assistant Director of Informatics is accountable to, and reports to the Director of Performance and Reform, and in conjunction with other operational Assistant Directors is responsible for the delivery of the strategic and operational management of the Information Governance Management agenda. He/she is also the Trust Data Protection Officer (DPO) and is responsible for ensuring that the Trust processes the personal data of staff, patients and service users in compliance with the applicable data protection legislation, regulatory requirements and best practice.

8.4 The Head of Information Governance is responsible for:

- ensuring compliance within data protection legislation and good practice within the organisation;
- progressing the Information Governance Strategy and Framework;
- providing guidance and advice to staff in relation to compliance with the relevant legislation; and
- reporting via the adverse incident reporting process on any breaches of Data Protection legislation.

8.4 Directors, Assistant Directors and Heads of Service are responsible for information held manually and electronically within their department. As Information Asset Owners their responsibilities include:

- informing the Head of Information Governance of any changes in the processing of personal data;
- identifying and justifying how sets of data are used;
- identifying all personal data for which they are responsible; and
- agreeing who can have access to the data.

8.5 All Trust staff including volunteers, temporary staff, agency, bank staff, and locums and also those staff contracted to carry outwork on behalf of the Trust have a responsibility to abide by the principles contained within this document and to adhere to the associated procedural guidelines. Further responsibilities include:

- observing all guidance and codes of conduct in relation to obtaining, using and disclosing personal information;
- observing all information sharing protocols in relation to the disclosure of information;
- obtaining and processing personal information only for specified purposes;
- only accessing personal information that is specifically required to carry out their work;
- recording information accurately in both manual and electronic records;
- ensuring any personal information held is kept secure; and
- ensuring that personal data is not disclosed in any form to any unauthorised third party.

9. Legislative Compliance, Relevant Policies, Procedures and Guidance

Staff must comply with relevant legislation, professional standards and guidance and other DoH publications as follows:

- Data Protection Act 2018
- The UK General Data Protection Regulation
- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order (Northern Ireland) 1925
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health records (NI) Order 1993
- Human Rights Act 1998
- Computer Misuse Act 1990
- The Common Law Duty of Confidentiality
- The Code of Practice on the Confidentiality of Service User Information
- DoH Good Management, Good Records
- Northern Ireland Records Management Standard (PRONI)

- Controls Assurance Standard
- ISO 15489 International Standard on Information and Documentation – Records Management

Relevant Trust Policies and Procedures

- Information Governance Policy
- Information Technology Security Policy
- Data Quality Policy
- Records Management Policy
- Clear Desk Procedure
- Policy for the Safeguarding Movement & Transportation of Patient/Client/Staff/Trust Records Files and Other Media Between Facilities
- Information Security Data Transfer – All User Standard
- Email Encryption Guidance
- Social Media Policy
- Disciplinary Policy and Procedure

10. Equality and Human Rights Consideration

This policy has been screened for equality implications as required by Section 75 and Schedule 9, of the Northern Ireland Act, 1998. Equality Commission for Northern Ireland Guidance states that the purpose of screening is to identify those policies which are likely to have a significant impact on equality of opportunity so that greatest resources can be devoted to those.

Using the Equality Commission's screening criteria; no significant equality implications have been identified. The policy will therefore not be subject to an equality impact assessment.

Similarly, this policy has been considered under the terms of the Human Rights Act, 1998, and was deemed compatible with the European Convention Rights contained in the Act.

Alternative Formats

This document can be made available on request in alternative formats, e.g. plain English, Braille, disc, audiocassette and in other languages to meet the needs of those who are not fluent in English.

11. Review of Policy

The Trust is committed to ensuring that all policies are kept under review to ensure that they remain compliant with relevant legislation.

This policy will be reviewed in January 2026 by the Head of Information Governance.

12. Sources of Advice and Further Information

Information Commissioner Office <https://ico.org.uk/>

[-NHS Digital - Information Governance Alliance](#)

Appendix 1

Special Category and Criminal Offence Personal Data Processed in Accordance with Schedule 1 of the Data Protection Act 2018

This appendix when read in conjunction with the rest of the General UK Data Protection Regulation and Data Protection Act 2018 Policy has been developed to meet the requirements in the Data Protection Act 2018 to have an appropriate policy document in place to process special category data and criminal offence personal information.

Schedule 1 part 1 of the Data Protection Act 2018 states that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security, or social protection.

It also meets the requirements at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The Trust relies on DPA Schedule 1 conditions to process special categories data and criminal offence information for example:

Schedule 1, Part 1, para 1 (employment and social protection), where the Trust needs to process Special Category/Criminal Offence data for the purposes of performing its obligations or rights as an employer, or for guaranteeing the social protection of individuals

- Processing personal data concerning health in connection to the Trust rights under employment law
- Providing human resources and occupational health facilities for employees
- Processing data relating to criminal convictions in connection with recruitment, discipline or dismissal

Schedule 1, Part 1, para 2 (Health or Social Care Purposes), where the Trust needs to process Special Category data for the delivery of health and social care purposes including the management of health care systems or social care systems or services.

Schedule 1, Part 1, Para 4 (Research etc), where the Trusts needs to process Special Category data for archiving, scientific, researching or statistical purposes.

Substantial Public Interest Processing

The specific conditions under which data may be processed for reasons of substantial public interest are set out in paragraphs 6 to 28 of Schedule 1 of the Data Protection Act 2018.

Schedule 1, Part 1, para 6 (statutory purposes), where the Trust needs to process Special Category/Criminal Offence data to comply with our statutory obligations.

Schedule 1, Part 2, para 8 (equality of opportunity), where the Trust needs to process Special Category/Criminal Offence data for the purposes of monitoring equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained.

Schedule 1, Part 2, para 10 (preventing or detecting unlawful acts), where the Trust needs to process Criminal Offence data for the purpose of preventing or detecting unlawful acts and obtaining consent would prejudice those purposes, and the processing is necessary for reasons of substantial public interest.

Schedule 1, Part 2, para 11 (protecting the public from dishonesty), where the Trust needs to process Criminal Offence data to protect members of the public from malpractice, unfitness, incompetence or mismanagement in the administration of a body or organisation, and obtaining consent would prejudice the exercise of the protective function, and the processing is necessary for reasons of substantial public interest.

Schedule 1, Part 2, para 12 (Regulatory requirements relating to unlawful acts and dishonesty), where the Trust needs to process Criminal Offence data to comply with a requirement which involves taking steps to establish whether an individual has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct, and the processing is necessary for reasons of substantial public interest.

Schedule 1, Part 2, para 14 (preventing fraud), where the Trust needs to process special category or Criminal Offence data to comply with a requirement that involves taking steps to prevent fraud or discloses personal data in accordance with arrangements made by an anti-fraud organisation eg Northern Ireland Audit Office National Fraud Initiative.

Schedule 1, Part 2, para 17 (counselling), where the Trust needs to process Special Category/Criminal Offence data in order to provide confidential counselling, advice or support or of another similar service provided confidentially, only where, in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining consent would prejudice the provision of the service, and the processing is necessary for reasons of substantial public interest

Schedule 1, Part 2, para 18 (safeguarding), where the Trust needs to process Special Category/Criminal Offence data in order to protect the physical, mental or emotional well-being of an individual under the age of 18, or over the age of 18 and at risk, only where, in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining the data subject's consent would prejudice the provision of the protection, and the processing is necessary for reasons of substantial public interest.

Schedule 1, Part 2 Para 21 (occupational Pensions) Where the Trust needs to process Special Category data in order to make a determination in connection with eligibility for, or benefits payable under an Occupational Health Scheme.

Steps taken to ensure compliance with Article 5 of the Data Protection Act are detailed in section 7 of this Policy.

Other relevant policies, procedures and guidance are listed under section 9 of this Policy.

Retention and erasure of personal data

We will ensure, where special category personal data is processed that:

- there is a record of that processing and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- where we no longer require special category data for the purpose for which it was collected, we will delete it, confidentially dispose of it, or render it permanently anonymous
- data subjects receive full privacy information about how their data will be handled and that this will include the period for which the personal data will be stored or if that is not possible, the criteria used.

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities
- Maintaining documentation of our processing activities (ROPA)
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high risk processing

We regularly review our accountability measures and update or amend them when required.