The Tavistock and Portman
NHS Foundation Trust

Data Protection Policy

Version:	1.0
Bodies consulted:	DSP Sub Committee of IGC, Caldicott Guardian, Director of HR & Corporate Governance, EMT
Approved by:	EMT
Date Approved:	25 June 2020
Lead Manager	Assistant Director of IG and Data Security & DPO
Lead Director:	Senior Information Risk Owner (Deputy CEO and Director of Finance
Date issued:	25 June 2020
Review date:	October 2024
Document Reference:	ISP:001 Data Protection Policy
Classification	OFFICAL
Intranet	Yes
Website	Yes

This policy replaces the previous Data Protection Procedure

Contents

1. Introduction 3
2. Purpose 3
3. Scope and applicability 3
4. Definitions 4
5. Policy Statements 4
    - Data Controller 4
    - Data Processor 4
    - Contractual obligations 4
    - Data Protection Impact Assessment 5
    - Lawful basis under the GDPR and Data Protection Act 2018 5
    - GDPR Principles 5
    - Data subject rights 6
    - Police requests for information 7
    - Retention of personal data 7
    - Obtaining communication preferences 7
    - Consent 8
    - PECR 8
    - PCI DSS 8
    - Incident Reporting 8
6. Duties and responsibilities 9
    - Data Protection Officer 9
    - Senior Information Risk Owner (SIRO) 9
    - Caldicott Guardian 10
    - Chief Clinical Information Officer 10
    - All staff responsibilities 10
7. Procedures 10
8. Training requirements 10
9. Process for monitoring compliance with this policy 10
10. References 10
11. Associated documents 11

Appendix: Equality Analysis 12

1. Introduction

1.1 The Trust needs to collect information about the people it deals with, including patients, students, staff and third parties such as contractors, suppliers and business contacts. Where the data we collect includes identifiable information about a living person (such as their name and address, NHS Number or National Insurance Number), this is personal information. Personal information includes items that on their own cannot identify an individual but could, when combined with other data available to the same recipient, lead to the identification of a living person.

1.2 Schedule 1 Part 2 of the Data Protection Act DPA 2018 states that where an organisation processes special category data, criminal offence data or employment, social security or social protection data, it must have an 'Appropriate Policy Document (APD)' to cover these processing activities. This is to meet the requirement under Schedule 1, Part 4 of the DPA 2018.

2. Purpose

2.1 This purpose of this policy is to meet the above legal requirement.

2.2 The policy sets out the Trust's requirements for compliance with its obligations under the Data Protection Act (DPA) 2018, the General Data Protection Regulation (GDPR), and associated laws and best practice, including the Privacy & Electronic Communications Regulations (PECR) and the Caldicott Principles.

3. Scope

3.1 This policy covers personal data. Personal data is recorded information from which a living person can be identified, either from the data alone, or when combined with other data that is or may become available to the recipient of the data.

3.2 This policy covers personal data about patients, parents/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.

3.4 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.

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

4. Definitions

Pseudonymised data	Data which has been deidentified, but from which the individual can be reidentified through a code or key.
Anonymised data	Data from which the risk of identification or reidentification is remote.
Data Controller	The organisation who legitimately determines the purpose of the processing of the personal data
Data Processor	A body or individual or processes data only on the instructions of the Data Controller
Data Subject	The (living) person who the information is about.

5. Policy Statements

Data Controller

5.1 The Trust is the Data Controller where it legitimately determines the purpose of the processing, that is, the reason why the processing is necessary.

Data Processor

5.2 Where the Trust processes data on behalf of another organisation (for example, under contract) it may be acting as a Data Processor.

Contractual obligations

5.3 When data is processed by a third party on behalf of the Trust (to comply with Article 28 of the GDPR), the Trust must ensure a data processing agreement/contract is in place that documents the Data Processor's obligations to the Trust as the Data Controller. This is to ensure that the Data Processor acts only in accordance the instructions of the Data Controller.

5.4 Where the Trust processes personal data on behalf of another data controller, it should do so only in accordance with an agreed data processing agreement.

5.5 Personal data should not be transferred outside of the EEA unless the European Commission considers the country 'adequate'. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. The ICO publishes standard contract clauses for data transfers outside of the EEA.

5.5.1 The Trust will review this section of the Policy as required following the UK's exit from the European Union.

Data Protection Impact Assessment

5.6 A Data Protection Impact Assessment (DPIA) is designed to help staff to systematically identify, analyse and minimise risks to people's privacy and is a key part of the Trust's accountability obligations under the GDPR. The DPIA does not have to eliminate all risks but should help minimise risks and/or determine whether the level of risk is acceptable in the circumstances. A DPIA template is available on the Trust's Intranet.

Lawful basis under the GDPR and Data Protection Act 2018

5.7 Personal data should only be processed where there is a lawful basis to do so.

5.8 The Trust must evidence which lawful bases it is relying upon under Articles 6 and 9 of the GDPR (General Processing and Special Category data respectively). Where relevant, the Trust must also evidence the Schedule 1 Conditions of Part 2 of the DPA 2018 and the additional safeguards under Part 4 of the DPA 2018. The Schedule 1 Conditions apply to those lawful bases under Article 9 which are in the 'substantial public interest'.

5.9 The lawful bases the Trust relies upon for each type of processing must be set out in the 'Record of Data Processing Activities' and included in the Trust's Privacy Notice. All staff should be familiar with the Trust's Privacy Notice and direct patients to it at appropriate stages. The Privacy Notice is kept under review and updated when there is any change to the Trust's processing activities.

5.10 Most of the Trust's processing activities are carried out under Article 6(e) Public task, i.e. where the data is processed 'in the exercise of official authority', or to perform a specific task in the public interest that is set out in law. Therefore, most of the Trust's processing activities are carried out under Part 2 of the DPA 2018.

5.10.1 With the lawful basis of Public task, the individual has a right to object to the processing and their objection should be complied with except where there is an overriding reason why the Trust needs to continue to process or retain the information.

5.11 Where the Trust discloses information to the Police, disclosure must meet a Condition under Schedule 8, Part 3 of the DPA 2018 (Law Enforcement Directive).

GDPR Principles

5.12 The GDPR sets out seven key principles, which the Trust must comply with:

- Lawfulness, fairness and transparency – the Trust must have a lawful basis for the processing. The processing must be fair and in line with the individual's reasonable expectations. All processing must be shown in the Trust's Privacy Notice.
- Purpose limitation – the Trust will only process personal data for the purpose(s) for which it was originally collected.

- Data minimisation – the Trust will only process personal data that is relevant, i.e. that is required for the purpose.
- Accuracy – the Trust will ensure that personal information is accurate and up to date. The Trust will provide opportunities for patients, students and staff to check the accuracy of the information we hold about them.
- Storage limitation – the Trust will hold personal data for as long as necessary, but no longer than is necessary. Staff should refer to the Trust's Retention Schedule.
- Integrity and confidentiality (security) – the Trust will ensure that the information it processes can be relied upon and is only available to staff who require access to carry out their role, using appropriate organisational and technical measures. Staff should refer to the Trust's 'Access Control Procedures'
- Accountability – the Trust is accountable for the protection of personal data and must be able to demonstrate compliance with data protection law.

Data subject rights

5.13 The GDPR provides the following rights for individuals, which the Trust must comply with.

- The right to be informed – individuals must be informed about the collection and use of their data. Staff should refer patients and students to the Trust's Privacy Notice at key stages, i.e. referral or application, discharge or end of course.
- The right of access/Subject Access Requests (SARs) – gives individuals the right to obtain a copy of the personal data we hold about them. Information for patients is available on the Trust's website. Requests from students should be emailed to Deansoffice@tavi-port.ac.uk. Requests for staff information should be addressed to the Director of HR & Corporate Governance.
- The right to rectification – individuals have a right to have information rectified if it is incorrect. If it is not agreed that the information is incorrect, the individual's comments should be added alongside the information that is disputed on the individual's record.
- The right to erasure – this applies where the lawful basis under Article 6 is Consent, Contract, Vital interests, or Legitimate interests. It does not apply where the lawful basis is Public task. Please refer to the Trust's Privacy Notice for the relevant lawful basis under Article 6.
- The right to restrict processing – an individual can ask for the information we process to be restricted.

- The right to data portability – this right applies where the lawful basis is Consent or Contract. The right does not apply with the lawful basis under Article 6 is Public task.
- The right to object – the individual can object to the processing and the Trust will consider their request. Where the Trust has no statutory obligation or overriding reason to continue the processing, the Trust will comply with the request.
- Rights in relation to automated decision making and profiling. Where the Trust makes decisions about individuals by automated means, the individual can request that the decision is reassessed by a person (human intervention).

5.14 For further guidance, please refer to ICO guidance on 'Individual rights' or email the Trust's Data Protection Officer at IG@tavi-port.nhs.uk.

Police requests for information

5.15 Requests for information from the Police should be handled in accordance with Schedule 8, Part 3 of the DPA 2018, the Law Enforcement Directive. Requests for information may be about patients, students, staff or third parties. Please refer to the Trust's procedures for dealing with information requests from the Police or contact the relevant lead for guidance.

Retention of personal data

5.16 The DPA 2018 requires the organisation to have a retention policy for how long it retains personal data for. Please refer to the Trust's Retention Schedule for further information.

Obtaining communication preferences

5.17 Patients/service users and students must be able to choose how they would prefer to receive communications (email, text, post or by phone) for each purpose. Except for electronic communications for marketing or fundraising purposes, consent under the GDPR is not required to send a communication. The GDPR lawful basis applies to the purpose of the processing and not the mode of communication.

5.18 Where the purpose of an electronic communication is marketing or fundraising, and the individual has not previously opted to receive these communications, then 'Consent' may be required to comply with the Privacy & Electronic Communications Regulations (PECR). If the purpose of the processing is outside of the Trust's official functions, and the processing is what an individual may reasonably expect, then the lawful basis of 'Legitimate interests' can be relied upon to send electronic marketing information.

5.19 Whilst marketing or fundraising information sent by post is not covered by PECR, for reasons of sensitivity, such communications should be captured within communication preferences.

5.20 People must be able to change their communication preferences easily and at any time.

Consent

5.21 Consent under the GDPR is only required for processing which falls outside of the Trust's official capacity and where the individual has not previously consented to their information being processed for the same purpose. For example, for the Trust to assist with a housing or benefit application, patient consent would be required to process their information for this purpose. It is important to note that consent under the GDPR includes a right to erasure and a right to withdraw consent. If the Trust cannot comply with a request for erasure, consent is not a valid lawful basis.

5.22 Common law consent (under the Common Law duty of Confidentiality) – this is not required for individual care where the information is processed in ways the patient could reasonably expect. Where the processing is beyond the patient's reasonable expectations, and there is no legal gateway for the processing, then consent should be obtained. The Common Law duty of Confidentiality is not a written law (it is based on case law), therefore, consent under common law does not provide the individual with a right to erasure.

PECR

5.23 As explained above, to comply with the Privacy and Electronic Communications Regulations (PECR), the individual's consent may be required to communicate electronically for marketing or fundraising purposes, i.e. if they have not previously opted to receive these communications.

5.24 If the individual has previously consented to receive these types of communications and if the processing is outside of the Trust's official functions, then the Article 6 lawful basis of 'Legitimate interests' may be relied upon instead.

PCI DSS

5.25 Where the Trust processes electronic payments, it must comply with the PCI DSS to ensure the protection of cardholder data.

Incident Reporting

5.26 Incidents involving the loss or potential loss of confidentiality or integrity of personal data, or that impact on the availability of data, should be reported via the Quality Management Portal. A new incident can be raised from within the Portal or from the Intranet.

5.27 Please refer to the Incident and Reporting Procedures for further guidance.

6. Duties and responsibilities

Data Protection Officer

6.1 As a public body, the Trust is required by the GDPR to appoint a Data Protection Officer (DPO). This policy establishes that role.

The DPO is responsible for monitoring compliance with the GDPR and DPA 2018. The DPO reports directly to the Board in relation to data protection matters. The DPO will work the Senior Information Risk Owner (SIRO) and the Caldicott Guardian to ensure that information security requirements and the Caldicott Principles (in respect of NHS patient data) are adopted.

6.2 The DPO will develop and maintain procedures to ensure compliance with data protection legislation, including:

- Maintaining a record of data processing activities
- Advising on Data Protection Impact Assessments (DPIAs)
- Ensuring compliance with Subject Access Requests
- Management of breaches of personal data
- Provision of privacy information
- Advice and guidance for staff
- Staff training on data protection
- Ensuring that responsibilities have been appropriately assigned
- To be the first point for data subjects about personal data
- To be the point of contact with the ICO
- Management of risks to the confidentiality and integrity of personal data

Senior Information Risk Owner (SIRO)

6.3 The SIRO's key responsibilities are:

- Leading and fostering a corporate culture that values, protects and uses information for the success of the organisation and benefit of its patients
- Owning the organisation's overall risk management policy and procedure, ensuring that information risks are assessed consistently by Information Asset Owners (IAOs).
- Advising the Chief Executive on the information risk aspects of their statement on internal controls.
- Owning the organisation's information incident management framework.

Caldicott Guardian

6.4 The Caldicott Guardian role has been a requirement for NHS bodies since 1998. The Caldicott Guardian is responsible for safeguarding the confidentiality of NHS patient information, ensuring that patient information is processed ethically and in line with the patient's reasonable expectations.

Chief Clinical Information Officer

6.5 The Chief Clinical Information Officer (CCIO) role is held by a practising clinician. The role combines medical expertise with the adoption of technology, ensuring that evidence-based informatics can be used to improve patient care.

All staff responsibilities

6.6 All staff must ensure they comply with requirements for the protection of personal data, whether about patients, applicants, students, staff or third parties.

6.7 All staff must complete and pass the mandatory annual NHS Data Security Awareness training. For employees, training is accessed and recorded via the Electronic Staff Record (ESR)

7. Procedures

- Procedure for handling requests for information under the General Data Protection Regulation/Data Protection Act 2018 and Access to Health Records Act
- Incident and Reporting Procedure

8. Training requirements

8.1 All staff must complete the annual NHS Data Security Awareness training.

8.2 Specialist roles should complete additional training on a regular basis, pertinent to their role. The DPO will ensure that staff in specialist roles and Board members receive data protection training and will maintain a record of staff data protection training across the organisation.

9. Process for monitoring compliance with this policy

9.1 Compliance with this policy will be monitored by the Trust's DPO, who will report to the Integrated Governance Committee (IGC) via the Data Security & Protection Workstream.

10. References

- General Data Protection Regulation (ICO)
- Data Protection Act 2018 (ICO)
- PECR (ICO)

11. Associated documents

- Privacy Policy
- ICT Security Policy
- Data Protection Impact Assessment Template
- Pseudonymisation and Anonymisation of Data Procedure
- Records Retention Schedule
- Risk Management Policy and Strategy
- Risk Management Procedure

Appendix: Equality Analysis

Completed by	**Assistant Director of IG and Data Security & DPO**
Date	**18 June 2020**

The following questions determine whether analysis is needed	**Yes**	**No**
Does the policy affect service users, employees or the wider community? The relevance of a policy to equality depends not just on the number of those affected but on the significance of the effect on them.		X
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?		X
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X