Data protection policy

1. Introduction

1.1 This document sets out the data protection policy for the Professional Standards Authority for Health and Social Care (‘the PSA’).

1.2 The PSA is a data controller and ’public authority’ for the purposes of data protection legislation.

1.3 This policy forms part of our strategy for handling personal data (and other sensitive information) and explains the rights and responsibilities of those handling personal data. All staff are contractually bound to comply with data protection and relevant PSA policies.

1.4 We aim to:

- Demonstrate the PSA's commitment to Data Protection Legislation (DPL) and the principles of data protection
- Outline how the PSA will work to comply with the DPL through technical and organisational measures and the principles of data protection by design and data protection by default.

1.5 This policy should be read in conjunction with:

- Data Protection Act – individual rights policy.

2. Scope

2.1 This policy applies to all personal data, in both electronic and paper form, held by the PSA, transferred to or exchanged with third parties, or held by third parties on behalf of the PSA.

2.2 Requirements on contractors will be set out in the contractual arrangements with them, or other notices given from time to time.

3. Roles and responsibilities

3.1 The ultimate responsibility for the PSA's compliance with DPA lies with the Chief Executive, in his role as Senior Information Risk Officer (SIRO).

3.2 The Head of Governance acts as the PSA's Data Protection Officer (DPO) and is responsible for advising the PSA on data protection matters.

3.3 The Information Asset Owners’s (IAO's), the Directors, for each of the three Directorates are responsible for ensuring compliance with data protection in their areas. This includes the requirement to take all reasonable steps to ensure third parties comply when processing personal data on behalf of the PSA. IAOs should contact the DPO or SIRO in the following circumstances:

- If they are unsure of the lawful basis which they are relying on to process personal data

- If they need to rely on consent for processing personal data
- If they need to prepare privacy notices or other transparency information
- If they are unsure about the retention period for the information being processed
- If they are unsure about what security or other measures they need to implement to protect personal data
- If they are unsure on what basis to transfer personal data outside the European Economic Area (EEA)
- When a data subject requests their data rights
- Whenever they are engaging in a significant new, or change in, processing activity which is likely to require a DPIA or plan to use personal data for purposes other than those for which it was originally collected
- If they plan to undertake any activities involving automated processing including profiling or automated decision-making
- If they need help with any contracts or other areas in relation to sharing personal data with third parties (including our contractors)
- If they are planning to share data with another organisation or person in a way which otherwise could affect individual rights.

4. Compliance

4.1 The PSA will make regular and ongoing mandatory training available to staff to promote understanding and compliance with the PSA's policies and procedures. Any further training or development needs will be assessed as necessary.

4.2 The PSA will regularly review the systems and processes under its control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

4.3 Any alleged breach of this policy may result in an investigation which may result in action being taken by the PSA including disciplinary procedures or, termination of a contract for services.

5. Policy review

5.1 We will review this policy annually, or more frequently in the event of any legislative or regulatory changes.

6. The data protection principles

6.1 To meet the requirements of the DPL the PSA will ensure personal data is:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)

- Collected only for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation)
- Accurate and where necessary kept up-to-date (accuracy)
- Not kept in a form which identifies data subjects for longer than is necessary for the purposes for which the data is processed (storage limitation)
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (security, integrity and confidentiality)
- Not transferred to another country without appropriate safeguards being in place (transfer limitation)
- Made available to data subjects and data subjects are allowed to exercise certain rights in relation to their personal data (data subject's rights and requests).

6.2 The PSA is responsible for, and must be able to demonstrate compliance with, the data protection principles listed above (accountability).

7. Processing and use of personal data, and the legal basis for processing data

Data protection legislation

7.1 The PSA will maintain a personal information audit log which sets out the processing activities under its responsibilities in accordance with the DPL.

7.2 The PSA primarily processes personal data about:

- Those working for and on behalf of the PSA
- Individuals assisting the PSA to discharge its functions
- External stakeholders and customers engaging with the PSA about the work it does, including those who wish to make a complaint about the PSA.

7.3 The lawful bases under the DPL for processing personal data by the PSA are generally because:

- We need to process the data for the performance of a contract with the data subject
- We need to process the data to comply with legal obligations on the PSA (and in particular our duties arising further to the National Health Service Reform and Health Care Professions Act 2002)
- We need to process the data for the performance of a task carried out in the public interest or in the exercise of official PSA vested in the PSA (and in

particular our functions arising further to the National Health Service Reform and Health Care Professions Act 2002)

7.4 Certain activities undertaken by the PSA may not be covered by the above conditions. In such circumstances, the PSA will record the alternative legitimising conditions under which it processes the personal data.

7.5 The PSA processes certain special category personal data. For example, in connection with its functions as an employer as well as to discharge certain core functions. In general terms, the legitimising conditions for such processing are:

- To perform or exercise obligations or rights of the PSA or the data subject for the purposes of employment
- To exercise the functions conferred on the PSA by an enactment (such as the National Health Service Reform and Health Care Professions Act 2002) and is necessary for reasons of substantial public interest
- To monitor and keep under review equality of opportunity or treatment by the PSA
- To prevent or detect unlawful acts, so that processing must be carried out without the consent of the Data Subject so as not to prejudice those purposes, and is necessary for reasons of substantial public interest;
- To protect the public against dishonesty, malpractice, unfitness or incompetence, so processing must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and is necessary for reasons of substantial public interest.

Confidentiality

7.6 A duty of confidence arises when information is provided for example, when a regulator passes on medical records of an individual to a member of staff.

7.7 To comply with obligations under the common law of confidentiality, the general principle is that information which is held by the PSA relating to individuals should not be used or disclosed except in accordance with the PSA exercising any function conferred on it by or under an enactment, in the public interests, or with the individual's consent (or within their reasonable expectations). A lack of ability to understand the likely use and disclosure of information does not diminish the duty of confidence.

7.8 In cases of doubt staff should discuss with the DPO, an IAO or the SIRO.

Transparency

7.9 General information about how the PSA processes personal data is available on our website. The PSA will also communicate fair processing information through correspondence or other material directed towards specific data subjects or groups of data subjects.

7.10 The PSA will ordinarily seek to provide fair processing information to data subjects at the time that the information is obtained, or within 30 days. In certain circumstances it may not be possible or appropriate to provide fair processing

information within that timeframe, for instance because we first need to review the information to properly discharge our functions.

7.11 The nature of its work may exclude the PSA from certain obligations to provide fair processing information, and to comply with other data subject rights, where the processing would prejudice the proper discharge of the PSA's functions. Similarly, we may not make fair processing information available where personal data is processed for the purposes of obtaining legal advice, legal proceedings (including prospective legal proceedings), or sharing information with the police or other law enforcement bodies.

Purpose limitation

7.12 The PSA will ensure that it collects data only for specified, explicit and legitimate purposes. The PSA will not further process data in any manner incompatible with those purposes.

7.13 Where the PSA intends to use data for another, different or incompatible purposes from that which was indicated when we first obtained the data,we will ensure that anytprivacy implications of the proposals have been assessed. We will theninform the data subject of the new purposes and that there is an appropriate legal basis for those purposes.

Data minimisation

7.14 The PSA will ensure that the personal data it processes are adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

7.15 Information must be deleted or securely destroyed as soon as they are no longer necessary in line with the PSA's retention policy.

7.16 Staff must only process personal data as required for their role.

Accuracy

7.17 The PSA will ensure that as far as reasonable the personal data it holds is accurate and, where necessary, kept up-to-date.

7.18 Staff are responsible for checking the accuracy of any personal data at the point of collection and at regular intervals afterwards. Staff must take all reasonable steps to destroy or update inaccurate or out of date personal data.

7.19 From time to time we may receive information which is (or appears to be) factually inaccurate, or an opinion which someone disagrees with. We may continue to hold copies of such information as part of our functions.

Storage limitation, retention and destruction

7.20 The PSA will ensure that personal data is not kept in an identifiable form for longer than is necessary for the purposes for which the data is processed in line with its retention policy.

Security, integrity and confidentiality

7.21 The PSA has appropriate safeguards to protect the personal data we process against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

7.22 The PSA's staff and contractors must comply with the *Removing document and IT user policy* and *Protecting personal and sensitive data policy*, which sets out the measures that must be taken to protect the confidentiality, integrity and availability of all personal data from the point of collection to the point of destruction.

Security incidents

7.23 Anyone involved in or witness to an information security incident (or suspected incident), including risk of a breach must raise these concerns with the DPO, an IAO or the SIRO as soon as possible after becoming aware of it. Incidents may be notified by any employee of the PSA, a supplier or anyone working for or on behalf of the PSA.

7.24 Information security incidents must be reported and managed in accordance with the PSA's *Guidance on the reporting of unclassified and classified data breaches*.

Transfer limitation

7.25 The PSA will only transfer data outside the EEA where it is necessary to fulfil the PSA's functions, is necessary in the public interest, the data subject has explicitly consented to the transfer or because the transfer is necessary for the establishment, exercise or defence of legal claims.

Data subject's rights and requests

7.26 Anyone wishing to exercise their right to request access to personal data that that the PSA holds about them should make the request in writing to the DPO.

7.27 Any Data Subject request received must be sent at the earliest possible time to the DPO and handled in accordance with the PSA's *Individual Rights policy*.

Privacy by design

7.28 The PSA will consider and where appropriate implement appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy by design principles.

Data protection impact assessments

7.29 The PSA will consider the need for, and where necessary conduct, Data Protection Impact Assessments (DPIAs) when processing any personal data in line with its policy on DPIAs.

7.30 The PSA will conduct a DPIA (and discuss the findings with the Data Protection Officer) where it is undertaking a new processing activity and where this might

constitute a risk to the rights and freedoms of any body who is the subject of this data processing.

7.31 Any DPIA must be completed using the DPIA template. The record of the DPIA must be filed with the Data Protection Officer.

Automated processing and decision-making

7.32 Generally, the PSA does not engage in automated processing/profiling, or automated decision-making.

7.33 Where the PSA does engage in automated decision making/profiling, we will take steps to inform the data subject of why we feel this the decision-making or profiling is necessary, the significance of it any any likely consequences and give the data subject the right to intervene, express their point of view or challenge the decision. Where possible the PSA will do this prior to the decision being taken.

7.34 A DPIA must be carried out before any automated processing (including profiling) or automated decision-making activities are undertaken.

Data processors

7.35 The PSA may contract with other organisations to process personal data on its behalf.

7.36 Decisions to engage a data processor(s) must be taken following due diligence on the proposed processor, to establish that the processor can provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of DPL.

Data sharing and disclosure

7.37 Personal information must not be disclosed outside of the PSA unless:

- It is consistent with our policy on removal of documents and IT containing personal and sensitive data policy and the obligation of fair processing
- It is necessary for the PSA to exercise any of the functions conferred on it by or under any enactment
- It is otherwise is fair and lawful and complies with Data Protection Legislation; or
- The Data Subject has given his/her consent to the disclosure.

7.38 When seeking consent from an individual, they must be informed of the reason for the disclosure and to who the disclosure is going to be made. Consent should only be sought if there is a genuine and fair choice for the data subject on the matter in question. Where consent is not sought, it may still be appropriate to invite their views on disclosure.

7.39 In all cases no more information will be disclosed than is necessary to achieve the purpose behind the disclosure. In any cases where the data subject has not given his/her consent to the disclosure, the matter must be referred to the DPO, an IAO or the SIRO prior to disclosure of the data.

7.40 Generally personal information should not be disclosed other than in accordance with this policy. It is accepted, however, that transfers may be necessary on rare occasions. If personal information is to be transferred outside the PSA in circumstances that are not covered by the policy, then permission should be sought from the DPO, an IAO or the SIRO as soon as possible and the reasons for the disclosure entered into the disclosure log.

7.41 Under no circumstances is personal information to be transferred to a country or territory outside the EEA without the PSA of the SIRO (or delegated person in his absence).

8. Complaints procedure

8.1 Anyone who considers that this policy has not been followed may make a complaint to the PSA's DPO. This can be done by emailing Suzanne.dodds@professionalstandards.org.uk or writing to;

The Professional Standards Authority
16-18, New Bridge Street, London, EC4V 6AG
Telephone: 020 7389 8030
Fax: 020 7389 8040

8.2 If you remain dissatisfied, you have the right to refer the matter to the Information Commissioner. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625 545 745
Fax: 01625 524 510
Email: enquiries @ico.gsi.gov.uk

9. Appendix A: Definitions

Data Protection Legislation	From 25 May 2018 the General Data Protection Regulation (GDPR) together with the Data Protection Act 2018 (the Data Protection Legislation) governs the processing of Personal Data. The Data Protection Legislation requires that Personal Data including Special Categories of Personal Data, which are regarded as more sensitive, must be processed by Data Controllers in accordance with the data protection principles set out in the GDPR.
Data Controller	A natural or legal person, public PSA, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. The PSA is

	a Data Controller for the purposes of Data Protection Legislation
Data Processor	Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.
Data Subject	Any living individual who is the subject of Personal Data.
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. The above definition includes any expression of opinion about the individual and any indication of the intentions of the Data Controller (i.e. the PSA) or any other person in respect of the individual.
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.
Special catergories of Personal Data (formerly "sensitive personal data"	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Information about the commission of offences or criminal proceedings is also regarded as sensitive under Data Protection Legislation and we handle such information commensurately.

Version Control

Version	Status	Description of Version	Date Completed
1.0	Draft	Data protection policy	15/05/2018
1.1	Approved	Data protection policy	17/07/2018
1.2	Approved	Amendments to improve usability	09/18
1.3	Approved	Annual IAO review no change	Nov 2020
1.4	Approved	Updated contact details	Nov 2023