

Information Governance Policies for Staff and Stakeholders

Contents

Information Governance Policies - Your rights (internal and external facing)

1. Data protection policy	3
2. Data Protection Legislation – Individual rights	13
3. Freedom of Information Policy	26
4. Information risk policy	32
5. Privacy Notice	37

The documents contained within this handbook have been collated for ease of reference. However, each document forms a policy in its own right and can be read individually.

1. Data protection policy

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 legislation 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.

Scope

- 1.5 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.
- 1.6 Requirements on contractors will be set out in the contractual arrangements with them, or other notices given from time to time.

Roles and responsibilities

- 1.7 The ultimate responsibility for the PSA's compliance with DPL lies with the Chief Executive, in their role as Senior Information Risk Officer (SIRO).
- 1.8 The Head of Governance acts as the PSA's Data Protection Officer (DPO) and is responsible for advising the PSA on data protection matters.
- 1.9 Each Director is the Information Asset Owner (IAO), for their Directorate and 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.

Compliance

- 1.10 The PSA will make regular and ongoing mandatory training available to staff, at least once a year, to promote understanding and compliance with the PSA's policies and procedures. Any further training or development needs will be assessed as necessary.
- 1.11 The PSA will regularly review the systems and processes under its control to ensure that 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.
- 1.12 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.

The data protection principles

- 1.13 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).

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

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

Data protection legislation

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

1.16 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.

1.17 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 authority vested in the PSA (and in particular our functions arising further to the National Health Service Reform and Health Care Professions Act 2002)

- 1.18 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.
- 1.19 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

- 1.20 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.
- 1.21 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 interest, 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.
- 1.22 In cases of doubt staff should discuss with the DPO, an IAO or the SIRO.

Transparency

- 1.23 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.

- 1.24 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.
- 1.25 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.
- 1.26 As part of its statutory functions under the National Health Service Reform and Health Care Professions Act 2002, the PSA may publish section 29 court judgments and consent orders on its website.
- 1.27 Before publication, the PSA will consider:
- Whether publication is necessary and proportionate;
 - Whether any personal data should be anonymised or redacted;
 - Whether any special category personal data should be redacted;
 - Any restrictions imposed by a court; and
 - its obligations under data protection legislation.
- 1.28 Further information is available in the PSA's Privacy Notice and publication guidance.

Purpose limitation

- 1.29 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.
- 1.30 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 any privacy implications of the proposals have been assessed. We will then inform the data subject of the new purposes and that there is an appropriate legal basis for those purposes.

Data minimisation

- 1.31 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.
- 1.32 Information must be deleted or securely destroyed as soon as they are no longer necessary in line with the PSA's retention policy.

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

Accuracy

- 1.34 The PSA will ensure that as far as reasonable the personal data it holds is accurate and, where necessary, kept up-to-date.
- 1.35 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.
- 1.36 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

- 1.37 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

- 1.38 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.
- 1.39 The PSA's staff and contractors must comply with our policy on '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. This policy can be found within our 'Information Governance Policies for Staff' and is available to the public on request.

Security incidents

- 1.40 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.
- 1.41 Information security incidents must be reported and managed in accordance with the PSA's 'Guidance on reporting data breaches'.

Transfer limitation

- 1.42 The PSA will only transfer data outside of the UK 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

- 1.43 Anyone wishing to exercise their right to request access to personal data that the PSA holds about them should make the request in writing to the DPO.
- 1.44 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

- 1.45 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

- 1.46 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.
- 1.47 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 anyone who is the subject of this data processing.
- 1.48 A Data Protection Impact Assessment must be completed before implementing, or making any material change to the PSA's policy on publication, retention, anonymisation or removal of section 29 court judgments or consent orders.
- 1.49 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

- 1.50 Generally, the PSA does not engage in automated processing/profiling, or automated decision-making.
- 1.51 If 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 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.
- 1.52 A DPIA must be carried out before any automated processing (including profiling) or automated decision-making activities are undertaken.

Data processors

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

- 1.54 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

- 1.55 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 their consent to the disclosure.
- 1.56 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.
- 1.57 No more information will be disclosed than is necessary to achieve the purpose behind the disclosure. In cases where the data subject has not given their consent to the disclosure, the matter must be referred to the DPO, an IAO or the SIRO prior to disclosure of the data.
- 1.58 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 with the reasons for the disclosure entered into the disclosure log.
- 1.59 Under no circumstances is personal information to be transferred to a country or territory outside the UK without the PSA of the SIRO (or delegated person in his absence).

Publication of Personal Data

- 1.60 Publication of information by the PSA, including publication on its website, constitutes processing of personal data where an individual can be identified.
- 1.61 Before publishing court judgments, consent orders or other regulatory documents, the PSA must consider:
- The lawful basis for publication;
 - Whether publication is necessary for its statutory functions;
 - Whether publication of identifying details is proportionate;

- Whether redaction or anonymisation is appropriate; and
- Whether a DPIA is required.

Complaints procedure

- 1.62 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

- 1.63 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: -0303 123 1113

The Information Commissioner can also be contacted via the ICO's website through a web form and live chat. More information regarding this can be found here:
<https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Appendix A: Definitions

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 categories 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.
---	---

2. Data Protection Legislation – Individual rights

Purpose

- 2.1 This document sets out our policies on the rights of individuals under Data Protection Legislation (DPL). The individual rights covered in this policy are:
- The right to be informed
 - The right of access (subject access requests)
 - The right to rectification
 - The right to erasure
 - The right to restrict processing
 - The right to data portability
 - The right to object
 - Rights in relation to automated decision making and processing.
- 2.2 The General Data Protection Regulation (GDPR) together with the Data Protection Act 2018 (the Data Protection Legislation) sets out the responsibilities of those dealing with personal data and the rights of individuals to access their personal data. All staff (including temporary staff), contractors and any third party working on behalf of the PSA are contractually bound to comply with the Data Protection Legislation (DPL) and other relevant the PSA policies.
- 2.3 The PSA will provide staff with appropriate training so that they are able to comply with their responsibilities under this policy.

Please send any requests in relation to individual rights or for more information to the Head of Governance at suzanne.dodds@professionalstandards.org.uk

Introduction

- 2.4 DPL gives you the right to confirmation that your data is being processed, to know what information is held about you, how that information is processed, and receive access to this data. It provides a statutory framework to ensure that personal information is handled properly.

- 2.5 The purpose of allowing access to personal data is so that you are aware of and can verify the lawfulness of the processing.

What is personal data

- 2.6 Personal data means any information relating to an identified individual 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. This 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.
- 2.7 This applies to both information held electronically and manually.

Right to be informed

- 2.8 The PSA is committed to being transparent over how we use personal data.
- 2.9 We inform people how we use their personal data through our privacy statement set out in section 5 below. We may make other information available depending on the circumstances.
- 2.10 Information about how to make a request will be published on the PSA’s website. We will keep under review what other materials may reasonably be made available to inform Data Subjects about how to exercise rights under DPL.

Right of access (subject access request)

What is the PSA’s general policy on providing information?

- 2.11 We welcome the rights of access to information set out in the DPL. We are committed to operating openly and to responding all requests for information. We therefore welcome ‘informal’ requests and these may be a quicker and more effective way for you to access particular information. We will explain to you whether we are able to comply with any particular request.
- 2.12 If you wish to make a ‘formal’ subject access request, in accordance with the provisions of the legislation, we will provide you with:
- Confirmation that your data is being processed
 - Access to your personal data
 - Other supplementary information, as set out in Data Protection Legislation.

How do you make a right of access (subject access request)?

- 2.13 A subject access request (SAR) must be made in writing, we will require you to provide your full name and a contact address (either a postal address or an email address).
- 2.14 In order to ensure that we are able to process your request without delay it may be helpful to provide the following information with your request:
- Your full name, address and contact telephone number
 - Any information used by the organisation to identify or distinguish you from others of the same name (account numbers, unique ID's etc)
 - Details of the specific information you require and any relevant dates.
- 2.15 The PSA recognises that individuals may initially seek to exercise their subject access rights in a range of different ways (including by writing, telephone and email). However, because of the statutory requirement to be satisfied as to the applicant's identity (and to maintain an audit trail in connection with a request), the PSA will ordinarily ask any prospective applicant to provide written confirmation (via email or letter).

Confirmation of Identity

- 2.16 We routinely handle sensitive and confidential Personal Data, the processing and disclosure of which can be repercussive for the individuals concerned. Accordingly, we will not progress a SAR until it is satisfied as to the applicant's identity. We may ask for copy of a passport, driving licence, bank statement or other proof of identity.
- 2.17 Where the PSA is otherwise satisfied as to the identity of the person making the request (for instance if a request were made by a current employee), we may elect to waive the requirement for the applicant to provide proof of identity. The decision to waive proof of identity will be taken by the Head of Governance.

What is the timeframe for responding to subject access requests?

- 2.18 We will log the date the request was received (and the applicant's identity confirmed).
- 2.19 We will seek to provide you with the information as soon as possible and not later than one month of receipt. If a request is particularly complex or numerous requests have been submitted, we may extend the response time by up to two further months. However, if this is necessary, we will contact you within a month of your original request to advise you of this and to explain the reasons why. We will seek to provide as much information as possible as early as possible within that period and may make a 'staged' disclosure of information.

- 2.20 We will inform you without delay, and no later than one month after receiving the request, if we do not intend to take action in response to the request, including the reasons why the PSA does not intend to take action in connection with the request and the right to make a complaint with the ICO or seek a judicial remedy.

What do we do when we receive a subject access request?

Collation of information

- 2.21 We will undertake a reasonable and proportionate search for the personal data requested, in conjunction other relevant staff who will be responsible for assisting the team to locate and extract any relevant personal data.
- 2.22 We will check that we have enough information to find the information you have requested. If we feel we need more information in order to clarify the request, then we will promptly ask you for this.
- 2.23 Where we are processing a large amount of information about you, we may ask to specify the information the request relates to.

Issuing our response

- 2.24 Once any queries that the PSA may have around the information requested have been resolved, a copy of the information will be provided to you.
- 2.25 Before sharing any information that relates to third parties, we will where possible anonymise information that identifies third parties unless it is reasonable to disclose that information or we have their consent. Whilst the right under Data Protection Legislation is to “personal data”, rather than documents, we will, where appropriate, and as a matter of discretion, try to provide you with contextual information or entire documents to help you understand your information.
- 2.26 We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.
- 2.27 Where we hold data about a Data Subject, the PSA’s response shall contain the following information:
- The purpose of the processing
 - The categories of the personal data concerned
 - The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
 - Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period

- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a supervisory authority
- Where the personal data was not collected from the data subject, any available information as to their source
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer
- An explanation of whether and why any exemptions have been applied to the Personal Data we hold.

2.28 Any preferences of the data subject will be taken into account in determining the format in which the information is disclosed. Where the request has been made through electronic means (including email), in the first instance we will communicate our response in an electronic format, using PDF or other commonly accessible formats to provide personal data.

2.29 Appropriate security measures will be taken to protect data during the course of its disclosure, included encrypted transfer mechanisms. Where possible, the information will be disclosed in a secure, readable electronic format to minimise costs, provide an audit trail, protect the environment, and to promote the security of the information. Any personal data disclosed via hard copy will be sent special delivery or by courier or on an encrypted electronic medium.

Will there be a fee?

2.30 Information will ordinarily be provided free of charge.

Are there any grounds we can rely on for not complying with a subject access request?

Exemptions

2.31 Once all relevant information has been located, the Governance team will review the data prior to disclosure and will be responsible for deciding whether any exemptions apply under Data Protection Legislation.

2.32 In accordance with exemptions provided under the Data Protection Legislation, the PSA may not comply with a SAR (in full or in part) in a number of circumstances. These include:

- Where the information sought is mixed data relating to the applicant and another identifiable data subject who cannot be anonymised and the PSA does not have the consent of the second data subject to release the information which also relates to them; and it is not reasonable in all the circumstances to disclose the information
- Where the disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, tax-collection or similar activities or counter-fraud issues
- Where the disclosure would prejudice regulatory functions
- Where the information comprises Personal Data in respect of which a claim to legal professional privilege could be maintained in legal proceedings
- Where the information comprises Personal Data that consists of the records of the intentions of the PSA in negotiations with the data subject, to the extent that that the disclosure would be likely to prejudice those negotiations
- Where the disclosure would cause serious mental or physical harm to the applicant or another person.

2.33 In assessing whether or not to disclose mixed data without consent, the PSA's starting point shall be non-disclosure. In weighing the extent to which any mixed data should be disclosed, the PSA will have regard to all the circumstances, including but not limited to the statutory factors of:

- The type of information that would be disclosed
- Any duty of confidentiality owed to the other individual
- Any steps taken by the PSA with a view to seeking the consent of the other individual
- Whether the other individual is capable of giving consent
- Any express refusal of consent by the other individual.

2.34 Other exemptions may also apply on a case by case basis.

Manifestly unfounded or excessive requests

2.35 If a request is manifestly unfounded or excessive, particularly if it is repetitive, the PSA can either charge a reasonable fee taking into account the administrative costs of providing the information or refuse to respond to the request.

2.36 Where we refuse to respond to the request we will explain why we have done so and advise of your right to complain to the ICO. We will do this without undue delay and within one month.

2.37 In deciding whether multiple requests are excessive (or made at unreasonable intervals), and what action to take in consequence, the PSA will consider all the relevant factors, including the following:

- The nature of the data (including whether it is particularly sensitive)
- The purposes of the processing, including whether the processing is likely to cause detriment to the requester
- The frequency with which the data is altered, including whether the data is likely to have changed or been altered since the previous request
- The time that has elapsed since the previous request
- The volume of information involved
- Any reasons given by the applicant for wanting the same information again
- Whether the information would be disclosable through other channels
- A record shall be kept of the PSA's decision making, and this explanation will be given to the applicant. The applicant may ask for a review of the decision.

What if you identify an error in our records (the right to rectification)?

- 2.38 If we agree that the information is inaccurate or incomplete, we will rectify it and where practicable, destroy the inaccurate information. Please note that a difference in opinion or interpretation is not the same as an inaccuracy, but we may record your disagreement with the data in question.
- 2.39 If we have disclosed the personal data in question to a third party, we will inform the third party of the rectification unless this is impossible or involves disproportionate effort. On request we will inform you of any third-party recipients.
- 2.40 We will respond to any request for rectification within one month although we reserve the right to extend this by two months where the request is particularly complicated.
- 2.41 If we do not agree the information is inaccurate or we cannot delete the information, we will make a note of the alleged error and keep this on file. We will also explain why this is the case and advise of your right to complain to the ICO and to a judicial remedy. We will do this without undue delay and within one month.

What if you want the PSA to stop processing your data and delete it (the right to erasure)?

What is the right to erasure

- 2.42 The right to erasure is also known as the 'right to be forgotten'. This is effectively the right to request the deletion or removal of your personal data where there is no compelling reason for the PSA to process (or continue to process it).

When does it apply

2.43 The right to erasure is not an automatic 'right to be forgotten' and your right to erasure only applies in certain circumstances. The circumstances to which it may apply are as follows;

- It is no longer being necessary for the purposes it was originally collected
- Where the PSA is relying on consent for processing and you withdraw this consent
- Where you object to the processing of your personal data and there is no overriding legitimate interest to continue with the processing
- The personal data was not processed in line with Data Protection Legislation and is therefore unlawful
- Erasure is necessary to comply with another legal obligation
- The personal data is processed in relation to the offer of information society services to a child (e.g. feedback collated via our social media accounts).

Situations where the PSA may refuse to consider a request

2.44 There are certain circumstances where the PSA may refuse to comply with a request. These may include the following:

- To exercise the right of freedom of expression and information
- Where the information is needed to comply with a legal obligation or for the performance of a task carried out in the public interest, including the PSA's statutory functions relating to public protection, public confidence in professional regulation and informing the public about the exercise of its statutory powers
- Where the information is for public health tasks in the public interest
- Where the information is for archiving for public interest or research purposes
- Where the information is held for defending legal claims.

How to apply

2.45 Should you wish to make such a request you should send us the request in writing. When we receive the request, we will send you written notice that either we have complied with your request, intend to comply with it or state the extent to which we will comply with it and why as soon as possible.

2.46 While the right to erasure is not limited to circumstances where processing causes unwarranted or substantial harm, it would help our considerations if you could provide details of any harm you believe it is or may cause when making your request.

- 2.47 Special care and consideration will always be given in relation to children's personal data and we may take legal advice when receiving such a request.
- 2.48 If we have disclosed the personal data in question to a third party we will inform the third party of the erasure unless this is impossible or involves disproportionate effort. On request we will inform you of any third party recipients.

Published Court Judgments and Consent Orders

- 2.49 The PSA may receive requests seeking removal, anonymisation or erasure of information contained within a published court judgment or consent order.
- 2.50 Requests will be considered on a case-by-case basis.
- 2.51 In determining whether publication should continue, the PSA will have regard to:
- The PSA's statutory functions and objectives
 - The public interest in publication
 - The age of the information
 - Whether the information remains relevant to public protection
 - Any evidence of harm or prejudice relied upon by the requester
 - Whether equivalent information remains publicly available from other sources
 - The rights and freedoms of the requester.
- 2.52 The starting position will generally be that continued publication remains lawful and justified where publication is necessary for the exercise of the PSA's statutory functions and duties.

What if you want the PSA to restrict the processing your data (the right to restrict processing)?

When does it apply

- 2.53 You also have a right to ask us to block or restrict processing of your personal data in some circumstances:
- Where you contest the accuracy of the personal data, we will restrict processing of this data until we can verify the accuracy
 - Where you object to the processing and we require time to consider whether the legitimate grounds for processing overrule this objection
 - Where the processing is unlawful but you oppose erasure and request restriction instead
 - Where we no longer require the personal data but you require it for another purpose such as to defend a legal claim.

What we will do

- 2.54 Where we restrict the processing of your data we will continue to store it but will not process it further.
- 2.55 We will hold a log with the minimum amount of information necessary to ensure that we continue to be able to restrict the processing in future for example where we are required to back up the system we may need to check our records to ensure no information is inadvertently added back onto mailing lists etc.
- 2.56 If we have disclosed the personal data in question to a third party we will inform the third party of the restriction unless this is impossible or involves disproportionate effort. On request we will inform you of any third party recipients.
- 2.57 If we decide to lift the restriction for any reason we will inform you in writing.

The right to data portability

What is the right to data portability?

- 2.58 The right of data portability is the right to request your information to reuse for your own purposes in a different environment. It effectively allows you to transfer your personal data from the PSA's IT environment to that of another organisation, securely and without hindering its usability.
- 2.59 In relation to the PSA's work it will be very rare for the right of data portability to apply.

When does it apply

- 2.60 The right to data portability applies where;
- You have provided the information to us
 - The processing is based on your consent (or for the performance of a contract)
 - When the process is carried out by automated means.

What we will do

- 2.61 Where you meet the requirements, we will provide your data free of charge, in a commonly used and machine-readable form.
- 2.62 We will provide the information within one month of your request except where your request is particularly complex or numerous requests have been submitted. In this case we may extend this by up to two further months. However, if this is necessary, we will contact you within a month of your original request to advise you of this and to explain the reasons why.
- 2.63 Where we are not taking any action in relation to your request we will write to you within a month to explain why and inform you of your right to complain

- 2.64 Where the data includes personal data relating to another party we will consider whether providing this data breaches their rights.

How to object to the PSA's processing of your personal data (the right to object)?

What is the right to object?

- 2.65 You have the right to object to any processing based on legitimate interests, the performance of a task in the public interest or exercise of official PSA or processing done for the purposes of research, or direct marketing
- 2.66 See our privacy notices or contact us for more information on the basis for processing.

Objecting on the grounds of legal tasks or the PSA's legitimate interests

- 2.67 Your objection must be on 'the grounds of your particular situation', please specify what this is when you make the request in order to help us to respond to your request.
- 2.68 We will stop processing the personal data unless:
- We have legitimate grounds for the processing, which override the interests, rights and freedoms set out in your request
 - The processing is for the establishment, exercise or defence of legal claims.

Objecting on the grounds of legal tasks or research purposes

- 2.69 Your objection must be on 'the grounds of your particular situation', please specify what this is when you make the request in order to help us to respond to your request.
- 2.70 Where the data processing is necessary for the performance of a public interest task we will consider whether it is necessary to continue processing it despite the objection.

Objecting on the grounds of direct marketing (newsletters etc)

- 2.71 We will stop processing your personal data on the grounds of direct marketing as soon as you request this.

What we will do

- 2.72 We will respond to your request within one month except where your request is particularly complex or numerous requests have been submitted. In this case we may extend this by up to two further months. However, if this is necessary, we will contact you within a month of your original request to advise you of this and to explain the reasons why.

- 2.73 Where we are not taking any action in relation to your request we will write to you within a month to explain why and inform to of your right to complain.
- 2.74 Where the data includes personal data relating to another party we will consider whether stopping processing providing this data breaches their rights.

Rights related to automated decision making

- 2.75 The PSA does not engage in “automated decision making”, which means decisions made about you solely by automatic means without any human involvement at all.

Checking of identity when we receive an individual rights request?

- 2.76 We will first check that we have enough information to be sure of your identity. Where the PSA is otherwise satisfied as to the identity of the person making the request (for instance if a request were made by a current employee), we may elect to waive the requirement for the applicant to provide proof of identity. However, if the PSA is not satisfied as to the identity of the requester it will take reasonable steps to identify the requester.
- 2.77 If an information request is received from a third party, the PSA will take whatever steps it considers reasonable to satisfy itself that the third party has the appropriate PSA to make the request.

If you are the parent/guardian of a child, we will need to consider whether the child can provide their consent to you acting on their behalf.

- 2.78 Audit and recording requestsThe PSA will maintain records of:

- The requests it receives
- The ‘raw’ products of any searches undertaken
- A master audit/redacted copy of the information proposed for disclosure
- Any correspondence with/the final response given to the applicant; and
- Any advice or other records received or prepared in the course of handling the request.

Our complaints procedure

- 2.79 If you are not satisfied with the way we have dealt with your individual rights request or any other action in relation to this policy you can seek recourse through our internal complaints procedure, the Information Commissioner or the courts.
- 2.80 The Chief Executive will deal with any written complaint about the way a request has been handled and about what information has been disclosed. The Chief Executive can be contacted at:

The Professional Standards Authority
16-18 New Bridge St, London EC4V 6AG
Telephone: 0207 389 8030

-
- 2.81 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: -0303 123 1113

The Information Commissioner can also be contacted via the ICO's website through a web form and live chat. More information regarding this can be found here:
<https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

3. Freedom of Information Policy

- 3.1 This document sets out the Professional Standards Authority's (the PSA's) policy on dealing with requests for information under the Freedom of Information Act 2000 (FOIA)

What is the FOIA?

- 3.2 The FOIA is intended to promote a culture of openness and accountability amongst public authorities by conferring on individuals a general right of access to recorded information. For the purposes of the FOIA, the PSA is a public Authority.
- 3.3 The FOIA places a duty on the PSA to provide information requested to the applicant, unless one of the exemptions set out in the FOIA applies.

What is the PSA's general policy to information requests?

- 3.4 The PSA welcomes the rights of access to information, set out in the FOIA¹. We are committed to operating openly and to dealing with requests for information about our activities. We have a publication scheme, through which some information about our activities can be obtained. If the information required cannot be found in our publication scheme, the guidance below, details how an information request can be made to the PSA.
- 3.5 Information routinely published by the PSA may include court judgments, consent orders and other documents relating to the exercise of the PSA's statutory functions. Publication of such information is governed by the PSA's information governance framework, privacy notices and data protection policies.

Guidance for the public

How do you make a request?

- 3.6 In order for your request for information to be valid it must:
- Be in writing (requests by email are acceptable)
 - State your name
 - State an address for correspondence (this can be an email address)
 - Describe the information in sufficient detail to enable us to identify what information has been requested.
- 3.7 When making your request you should specify how you would prefer to receive the information requested. The PSA will, as far as is reasonably practicable, provide the information to you in your requested format. If the PSA is unable to provide the information to you in your requested format, we will communicate the information by any means we consider reasonable in the particular circumstances of the request.

¹ Please note that whilst we are a UK wide organisation, because we are based in England we only abide by the requirements of the FOIA and are not bound by the Freedom of Information (Scotland) Act 2002.

What does the PSA do when we receive a request?

- 3.8 All requests for information are passed to the Governance team who will acknowledge receipt of the request, inform you of the date on which the 20 day time limit expires and will consider the request in further detail.

How will we manage the request?

- 3.9 The Governance team will work with the designated lead in the team holding the information to:
- Establish whether we hold the information
 - If the information is held, collate the information
 - Liaise with any third parties who provided the PSA with or would be affected by the release of the information
 - Consider whether any of the exemptions in the FOIA are applicable; and
 - Liaise with our legal adviser where necessary.
- 3.10 Once a decision has been reached on what, if any information can be disclosed, the Governance team will write to you.
- 3.11 We will as far as is reasonably practicable, disclose the information to you according to your stated preference. You must specify the preferred format; it is not sufficient to ask for information in 'all forms in which it is held'. If we cannot provide the information in the form you have requested, we will provide an explanation. If you have not stated a preference, then we may communicate the information by any means that are reasonable in the circumstances.

What do we do if we do not hold the information?

- 3.12 If you request information that we do not hold, we will
- Contact you and advise that we do not hold the information requested. If the information requested is held by another public Authority we will provide you with its contact details so you can forward the request to them.

What assistance and advice will we provide?

- 3.13 Section 16 of the FOIA places a duty on the PSA to provide advice and assistance, to individuals requesting information so far as it would be reasonable to expect us to do so. Advice and assistance may include the following:
- Explaining the types of information available
 - The format in which information is available
 - Information relating to our charging policy.
- 3.14 If we have difficulty in identifying the information you have requested, we will contact you to:

- Clarify the request
- Provide an explanation of our filing system; or
- If after taking reasonable measures to assist you in making your request, we cannot identify or locate the information we will disclose information we consider to be covered by your request along with an explanation of why we have disclosed what has been disclosed. We will also provide details of our complaint's procedure.

3.15 Where a request has been refused because of excessive costs, appropriate assistance will be provided explaining how the request could be refocused so that it could be complied with.

3.16 If you have made a request that spans both the FOIA and the Data Protection Act 2018 (DPA), we will inform you of this and deal with the requests separately and in accordance with the statutory time limits.

3.17 If we are unable to respond to your request within the statutory time limit, we will write to you explaining the delay and provide you with a new time scale for dealing with your request. If we are still unable to comply with the request within the new timescale we will write to you again with an update as to our progress in dealing with your request and provide you with a new timescale.

What is the timescale for responding to requests for information?

3.18 We will deal with requests for information promptly and in any event within 20 working days.

3.19 Where you have made a request, but it has not met the requirements of the FOIA, the 20-working day limit would not start until we had sufficient information to deal with the request.

3.20 Sometimes it is not possible to provide the information within 20 days, for example:

- Where we need to consider the public interest in disclosing the information; or;
- If we decide to charge a fee for processing the information, you are given three months from the date of our notice to pay. The 20-working day timeframe stops the day before the notice is sent and would restart the day after we receive the fee.

Will we charge for providing the information?

3.21 The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations provides that public authorities do not have to comply with a request where the cost of providing information exceeds £450 or 18 hours.

3.22 In considering whether responding to the request will exceed £450 we will take into account: the time taken to determine whether we hold the information, locating, retrieving and extracting the information.

3.23 If the request is estimated to cost more than £450, we can:

- Refuse to handle your request but offer advice and assistance on how to refocus the request to bring it within the acceptable limit; or
- Handle your request and charge a fee. You will be advised of the fee before the request is processed.

3.24 The fee will be based on:

- Any preference expressed by you in making the request as to the means or form of communication
- Reproducing any document containing the information; and
- Postage and other forms of transmitting the information.

3.25 The fee will only be charged if the costs are over £25.

Are there any grounds we can rely on for not complying with your FOIA request?

Vexatious or repeated requests

3.26 The FOIA says that we are not obliged to respond to a request for information if the request is vexatious. In determining whether a request is vexatious we will consider guidance issued by the Information Commissioner and relevant case law. In particular, we will consider:

- The intention of the requester
- The purpose or value of the request, particularly when the request is being made as part of a series of requests
- Whether the request can be characterised as obsessive or manifestly unreasonable.

3.27 Even if a request is not vexatious there is no obligation on the PSA to comply with a request which is identical or substantially similar to a previous request unless a reasonable interval has elapsed.

3.28 When considering whether a request is vexatious, we may seek legal advice.

Exemptions

3.29 There are a number of exemptions to the right of access. Exemptions are either qualified or absolute.

3.30 Where a qualified exemption applies the PSA must apply a two stage test. First, we must decide whether the exemption applies to the information requested and if it does, we will then apply the public interest test.

3.31 There are also a number of absolute exemptions. If an absolute exemption applies there is no need to consider the public interest.

The duty to confirm or deny

- 3.32 In all cases where a qualified exemption applies, and many cases where the exemption is absolute, we must also consider whether we can confirm or deny whether we hold the information.
- 3.33 This is a complex part of the FOIA and we may seek legal advice when before responding to the request.

Our obligations on refusal of a request

- 3.34 Where we refuse to provide information following a request or we cannot confirm or deny whether the PSA holds the information, we will issue a refusal notice setting out the reasons for the refusal.
- 3.35 If we rely on an exemption in not providing information requested, we will explain why we consider the exemption applies. If we rely on the public interest in not disclosing information requested, we will explain this in our refusal notice.
- 3.36 In any case, where we are withholding information, we will provide details to you of our complaint's procedure, and we will inform you of your right to complain to the Information Commissioner. Our complaints procedure and the Information Commissioner's details can be found below.
- 3.37 If you are unhappy with the way that we have handled your request, you can complain about us. Further information can be found on our website or by calling 0207 389 8030.
- 3.38 If you remain dissatisfied, you can contact the Information Commissioner at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: -0303 123 1113

The Information Commissioner can also be contacted via the ICO's website through a web form and live chat. More information regarding this can be found here: <https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

4. Information risk policy

Purpose

- 4.1 The purpose of this document is to define how the Professional Standards Authority for Health and Social Care (the PSA) delivery partners will manage information risk and how we will assess the effectiveness of our strategies and procedures on managing information risk.

Statement of Intent

- 4.2 Information is a key asset, and its proper use is fundamental to the delivery of our services. The public and our other stakeholders are entitled to expect that we will protect their privacy and use and handle information professionally and sensitively to ensure that their private information is protected. We will do this by effectively managing all risks, to the integrity, availability and confidentiality of our information whether held on paper or in our IT systems. Risks include inappropriate disclosure or non-disclosure of information, loss, theft or fraud, information being wrongly destroyed, staff acting in error, and a failure to utilise the information for the public good.
- 4.3 We see the benefits of managing these risks as being able to:
- Ensure that information is being used professionally and in line with all relevant guidance and legislation
 - Constrain threats to our information to acceptable levels so that we can maintain public confidence; and
 - Make informed decisions on when we should share or re-use information so that it can be used to its fullest value.
- 4.4 We have set down policies and procedures, which will enable the PSA, its employees and its delivery partners to work within an acceptable level of risk, and to be aware of when and whom to contact if they want to deviate from these policies, and the consequences both corporate and individual of not following these procedures.
- 4.5 The PSA's Executive Leadership team is committed to ensuring that all staff comply with this policy at all times.

Information Risk Management Structure

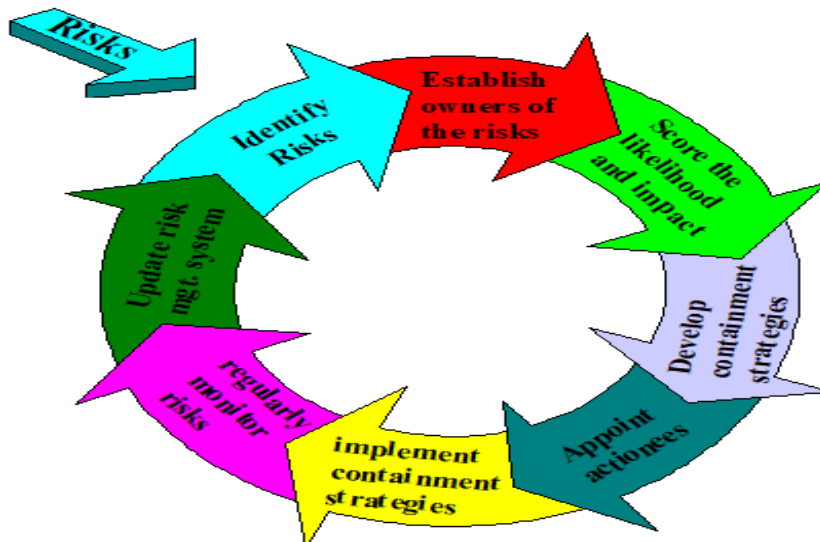
- 4.6 The PSA has put in place an information risk management structure to ensure that appropriate personnel have responsibility for the management of our information.
- 4.7 The PSA's Chief Executive is the Senior Information Risk Owner (SIRO) and is responsible for the management of information risk at Board level. He is responsible for:
- The overall information risk policy and risk assessment process
 - Ensuring that the policies and procedures are implemented, followed and agreeing any deviation from these

- Ensuring their effectiveness is tested
- Leading and fostering a culture that values, protects and uses information for the public good
- Reporting to the government on information risk management.

- 4.8 The team directors are the Information Asset Owners (IAOs). Their role is to understand what information is held, what is added and what is removed from our paper and electronic records, how information is moved and who has access to it and why.
- 4.9 As a result, they are able to understand and address the risks to their information, and ensure that information is fully used within the law for the public good. They are also able to provide written input to the SIRO annually on the security and use of their asset.
- 4.10 The Head of Governance is the PSA's appointed data protection officer.
- 4.11 All staff have the responsibility to manage their information in line with the PSA's record management and information risk policies and procedures. They also have the responsibility to notify the SIRO if there is a breach or a suspected breach of classified and unclassified information.

Information Risk Management Strategy

- 4.12 The risk management process for the PSA is shown below.



The Head of Governance and Information Asset Owners will discuss the risks related to the information we hold internally and that, which is shared or held with our delivery partners, when required. We collectively identify risks to our information, publication activities and information-sharing activities, agree how to either avoid these, or if that is not possible, manage and mitigate the adverse impact of these occurring.

- 4.13 Risks identified will be added to the PSA's risk register which is then reviewed by the PSA's Audit and Risk Committee and Board.
- 4.14 We pay considerable attention to managing risks and are prepared to take higher organisational risks to improve protection of patients and the public. Managers review risk on an ongoing basis and will tolerate, treat or avoid risks according to the nature of each risk.

Publication Risk

- 4.15 Where the PSA publishes court judgments, consent orders or other documents containing personal data, the PSA will assess the risks arising from publication including:
- Risks to the rights and freedoms of individuals
 - Risks associated with publication of special category personal data
 - Reputational risks
 - Risks associated with prolonged publication
 - Risks arising from failure to publish material relevant to public protection.
- 4.16 Such risks should be considered through the PSA's DPIA and risk management processes.

Threat Assessment

- 4.17 Our current risk assessment shows that the risks to our information are low. The risks to the information are being managed and where necessary this is documented in our risk register. We hold relatively little sensitive personal data and the access rights to this data are limited. We hold a register of staff that have access to these rights and this is regularly reviewed. Staff who have access to this are used to dealing with it appropriately and do so in accordance with our information security policies..

The Legal and Regulatory Requirements

- 4.18 When managing our information risk, the PSA works to the required legal and regulatory standards. Whilst this list is not exhaustive, they include:
- The Government's minimum mandatory measures
 - The Data Protection Act 2018
 - The General Data Protection Regulation 2018

- The Freedom of Information Act 2000
- The PSA's record management policies
- The PSA's policies on protecting personal and sensitive data
- The PSA's guidance on reporting, recovering from and managing a breach of information.

Building and protecting a culture where we value, protect and use information for public good

- 4.19 We have a culture where we value, protect and use information for public good. We reiterate regularly to staff the need to ensure that they adhere to The PSA's information governance policies. We have provided staff with information governance training.

Whistleblowing policy

- 4.20 We have a whistleblowing policy in place which states that a member of staff will be protected if they raise concerns under this policy about the unauthorised or inappropriate disclosure, misuse or loss of confidential, personal and / or sensitive information.

Reporting, Recovering and Managing from an Information breach

- 4.21 We have a policy in place, which sets out how The PSA will report, recover, and manage an information breach.

Corporate and individual consequences of the failure to adhere to information risk policies and procedures

Individual

- 4.22 We have a dismissal and disciplinary policy and procedure and acceptable IT usage policy, set out in the Employee Handbook, which incorporate the consequences of failing to adhere to the information risk policies and procedures.

Corporate

- 4.23 There could be significant consequences for the PSA as an organisation if we fail to adhere to our internal information risk policies and procedures. We could face considerable loss of reputation, particularly if there is media interest; we could face action by the Information Commissioner's Office or individuals if personal information was involved; we could face a loss of confidence by our stakeholders; and even a loss of people willing to work with us. Similar consequences could occur to our delivery partners.

Inspections

Internal

- 4.24 We conduct an annual assessment of the risks to the integrity, availability and confidentiality of our information within our organisation and with our delivery partners,nt which is recorded in our Annual Report. This is a comprehensive and objective report on the actions that we have taken in the year to manage our information risk, together with any outstanding issues that need to be addressed.

External

- 4.25 The PSA will comply with any reasonable external requests from the Information Commissioner's Office or others to inspect the implementation of our policies and procedures.

5. Privacy Notice

Purpose

- 5.1 This purpose of this notice is to tell you what you can expect when the Professional Standards Authority (the PSA) collects personal data. It includes information we collect about:
- Job applications and recruitment
 - Information about our staff
 - Expense claims
 - Complaint/share your experience information
 - Information in relation to a subject access request of Freedom of information request
 - Visitors to our website
 - People who subscribe to our newsletter
 - People who respond to a consultation/call for information
 - Information regarding people who attend our events
 - Information regarding fitness to practise cases
 - Performance review.
- 5.2 We are committed to safeguarding the privacy of your personal data. Your personal information will be held strictly in accordance with the Data Protection Act 2018 and the General Data Protection Regulation.
- 5.3 We will only collect the minimum information necessary to meet our stated purposes and this will be held securely in electronic format. Where information is sent physically, it will be scanned electronically, and hard copies destroyed securely in line with our retention and disposal policy.
- 5.4 If there is a specific need to retain an original or hard copy this will be stated clearly in this policy.

The Data Controller

- 5.5 The PSA is the Data Controller for any personal data you give to us. Suzanne Dodds is our Data Protection Officer. Suzanne's contact details are:

Suzanne Dodds
Professional Standards Authority
16-18, New Bridge St,
Blackfriars,
London,
EC4V 6AG
Telephone: 0207 389 8025
Email: Suzanne.dodds@professionalstandards.org.uk

The personal information we hold

Job applications and the recruitment process

What information we collect?

- 5.6 The PSA is (unless otherwise stated) the data controller for any information collected during the recruitment process.
- 5.7 We collect personal details including name and contact details, previous education and employment experience, referees and any other relevant information regarding your suitability for the role. You do not have to provide us with the information requested either at the application or interview stage. However, if you do not it may affect your application.
- 5.8 We will also ask you for information in relation to any disabilities. You do not have to provide us with the information requested. This will not affect your application.
- 5.9 We will request information regarding equality, diversity and inclusion (EDI). This will be on a voluntary basis and the form is detachable if people wish to post it anonymously. This will not affect your application.

Why we collect it?

- 5.10 The information collected during the recruitment process will only be used to process the application or to fulfil legal or regulatory requirements.
- 5.11 Information regarding disabilities will be used to consider the application under the guaranteed interview scheme or to make reasonable adjustments to assist you during any interview.
- 5.12 EDI data is collected for the purposes of reviewing our recruitment processes to ensure that they are open and fair, we use the data to ensure we are reaching a wide range of people and to review our recruitment approach to ensure that it is inclusive.

Do we share it with anyone?

- 5.13 We do not share information collected during the recruitment process with third parties or store it outside the EEA.
- 5.14 We ask for applications to be sent directly to our HR team who have responsibility for long listing. Shortlisted applications will also be shared with the internal recruitment panel.

- 5.15 Contact details, disability information and EDI information will be removed from the application before it is shared with the internal recruitment panel. However, they will be informed if you have applied under the guaranteed interview scheme in order to take this into account. It may be necessary to share details of reasonable adjustments requested for candidates selected for interview with the internal recruitment panel for the purposes of carrying these out.
- 5.16 This information will be recorded anonymously using a spreadsheet once entered the data will not be identifiable, no one outside of the HR team will ever have access to identifiable data and this will be securely destroyed as soon as it is entered into the system.
- 5.17 Information collected during the recruitment stage is collected for the purposes of assessing suitability for the post and to contact applicants whose application is being progressed.

Information about our current and former staff

What information we collect?

- 5.18 The PSA is (unless otherwise stated) the data controller for any information held about our current and former staff.
- 5.19 We hold the following information:
- Name and contact details
 - Emergency contact details
 - Proof of identity – we will ask you to bring original documents, and we will take copies
 - Reference information
 - Bank details
 - National insurance details
 - Pension information
 - Information regarding absences including sickness absence and family leave including Fit notes and MatB1 forms
 - Occupational Health information – there is no compulsory requirement for staff to attend OH. However, should you refuse to attend or release the information the PSA when asked then the PSA may need to reach a conclusion based on incomplete information. You will be given the opportunity to view the information before it is sent to the PSA

- Office attendance data - Sign-in data is collected automatically by Microsoft Entra ID when staff access PSA-managed devices or services. The data includes user identity (username), sign-in date and time, and source IP address. Information will only be collected to say whether someone is in the office or not on a given day and will not be able to identify locations outside of the office if staff are working remotely.
- EDI data (optional).

Why we collect it?

- 5.20 Your name and contact are held for the purposes of contacting you. This will only be used where there is a contractual necessity to send you information such as payslips or information about business continuity events.
- 5.21 Your emergency contact details are held so that we know who to contact in the event you have an emergency at work.
- 5.22 We are required by law to confirm your identity and proof of your right to work in the United Kingdom.
- 5.23 We hold references from your previous employer to determine your suitability for the role.
- 5.24 We hold bank details, national insurance details and pension information for the purposes of payroll. This is to ensure you are paid, are paying the correct NI contributions and pension contributions or to show that you have opted out and should not be paying pension contributions.
- 5.25 We collect information regarding absences to ensure that your statutory rights are protected including payments and leave.
- 5.26 We will use any medical information we are sent for the purposes of making reasonable adjustments.
- 5.27 Office attendance data is collected for the purposes of monitoring adherence to the hybrid working policy. It will not be used for the disciplinary purposes on its own but may be shared with the relevant line manager to conduct further investigations to ensure compliance with the hybrid working policy.
- 5.28 We will use EDI data for the purposes of;
- To ensure we are meeting our obligations under the Public Sector Equality Act Duty and enhance equal opportunities
 - To allow us to identify any gaps in our approach to EDI in the workplace which will allow us to ensure that every employee has the same access to training, development and other opportunities
 - To allow us to plan ahead such as allocating resources and budgets for things like training and development

- To allow us to identify areas where we are not performing at the level we are expecting and to use this information to help develop these areas with staff input such as targeted studies or focus groups and ensure that we enhance diversity across the PSA.

Do we share it with anyone?

- 5.29 Information collected regarding staff and former staff is held by the HR team.
- 5.30 Information relating to payroll or pensions is shared with the finance team.
- 5.31 Information relating to office attendance is held by the IT team.
- 5.32 Health information where relevant may be shared with your line manager, you will be asked for your consent before this is done.
- 5.33 The PSA uses data processors in relation to current and former members of staff. We have contracts in place with our data processors to protect your information and to ensure they cannot do anything with it without our permission. They will not share your information with third parties.
- 5.34 The PSA's HR and Payroll services are provided by Frontier. For more information on Frontier's privacy notice please see their website <https://www.frontier-ehr.com/our-privacy-policy/>
- 5.35 Occupational health services are provided to us by Capital Medical Services for more information on their privacy notices please contact hdavison@capitalmedicalsolutions.co.uk
- 5.36 The PSA is a data processor for NHS pensions. This means that we collect and process the information on behalf of NHS pensions but we do not control the information. NHS pensions is the data controller. Their privacy notice can be found here <https://www.nhsbsa.nhs.uk/privacy>
- 5.37 The PSA is a data processor for Standard Life pensions. This means that we collect and process the information on behalf of Standards Life pensions, but we do not control the information. Standards Life pensions is the data controller. Their privacy notice can be found here <https://www.standardlife.co.uk/privacy>

Expense claims

What information we collect?

- 5.38 If you wish to claim expenses from the PSA we request your name, contact details and bank details. You do not have to provide this information but if you do not we may not be able to pay your expenses.

Why we collect it?

- 5.39 This information is collected to pay the expenses and send you remittance advice.

Do we share it with anyone?

- 5.40 Personal information regarding expenses is held by the finance team. It is not shared with any third parties.

Complaint/share your experience information

What information we collect?

- 5.41 When you make a complaint about the PSA or share your experience about a regulator or an accredited register either by telephone, email or in writing we will create an electronic file. This may include file notes of the telephone call or scanned copies of original documents.
- 5.42 We will normally securely destroy hard copy documents after they are scanned in line with our policy on retention and disposal, unless you have specifically asked us to return the documents, you have included original documents, or we consider the information to be excessive. In these cases, we will return the documents through secure post explaining the reasons for this.
- 5.43 The file will normally include the name and contact details of the complainant and may include the names of any individuals included in the complaint.

Why we collect it?

- 5.44 If you are making a complaint about the PSA we will use the details, you have provided us with to process the complaint and to provide you with a response.
- 5.45 If you are sharing your experience about a regulator or accredited register, we may use your feedback to help inform our performance review of the regulator or our annual assessment of the accredited register. This will be done without identifying individuals.

Do we share it with anyone?

- 5.46 It may not be possible to investigate a complaint about an individual member of the PSA's staff without disclosing your details to them. This is to allow us to fully understand the complaint. If you wish to remain anonymous, we will try to respect this, but it may mean we are unable to investigate your complaint as fully as we would like.
- 5.47 As we do not have the power to investigate individual complaints raised under share your experience, we will not disclose your details to individual parties mentioned in your comments.
- 5.48 There may be occasions where we feel that it may be beneficial to contact a regulator or an accredited register on your behalf. In this case we will contact you setting out clearly what we intend to share, who we intend to share it with and what the purpose of the correspondence is. We will not share this until you have given us express consent to do so.

- 5.49 We may also use complaint/share your experience information to compile statistics such as the number of complaints received but this will not be done in a way which identifies you.

Information in relation to a subject access request (SAR) or Freedom of Information request (FOI)

What information we collect?

- 5.50 We will need to collect your name and a contact address (this could be either a postal or email address).
- 5.51 In the case of a subject access request, we may request enough information to verify your identity (see our Individual rights policy for more information).

Why we collect it?

- 5.52 Your name and contact details are collected for the purposes of contacting you in response to your request.
- 5.53 If we require information to verify your identity this will be used solely for the purposes of ensuring you are entitled to the information.

Do we share it with anyone?

- 5.54 Occasionally we may need to seek advice from external legal advisers on how to process your request. We will anonymise FOI requests. However, this may not always be possible in relation to SAR. This information will be treated in strictest confidence and in line with our contract with the legal advisers.
- 5.55 We will publish our responses to FOI requests on our website. However, we will not publish any identifiable data.

Visitors to our website

What information we collect?

- 5.56 When someone visits our website, we collect standard internet log information in relation to how they use the website such as what pages they visit.
- 5.57 The information is processed in a way that does not identify anyone, and we make no attempt to do so.
- 5.58 If we do ever want to collect personally identifiable information such as inviting people to take part in consultations, we will make this clear and explain what we intend to use the information for.

Why we collect it?

- 5.59 Website information is collected for us to identify what people are interested in and allow us to improve our website.

Do we share it with anyone?

- 5.60 We use a third-party site, Google Analytics to collect this information. We don't allow Google Analytics to make any attempt to identify users.
- 5.61 More details about this can be found in our 'Cookie policy'
<https://www.professionalstandards.org.uk/cookie-policy>

People who subscribe to our newsletter

- 5.62 Website captured personal data (PII) an external platform for storing data;
- Mailchimp – this emailing platform is being used to send out the email newsletter and similar content of significance. More information can be found here <https://eepurl.com/dyilK9>
 - Submission data collected by Drupal <https://www.drupal.org/privacy>

What information we collect?

- 5.63 When you subscribe to our newsletter we ask you to provide us with your name and email address. We may also ask you to provide your organisation name, job title, address and telephone number. This information is optional and you do not have to provide it. However, our newsletter is sent electronically and without an email address we will be unable to include you on our mailouts.

Why we collect it?

- 5.64 This information is collected to allow us to send you regular updates about our work.
- 5.65 You may unsubscribe from this at any time by emailing engagement@professionalstandards.org.uk

Do we share it with anyone?

- 5.66 We do not share details of our stakeholder networks with third parties.

People who respond to a consultation/call for information

What information we collect?

- 5.67 When you respond to a consultation, we ask you to provide us with your name and email address. We may also ask you to provide your organisation name, job title, address and telephone number. This information is optional, and you do not have to provide it. However, we may need to contact you to confirm details and verify information and if we are unable to contact you, we may need to put less weight on your response.

Why we collect it?

- 5.68 This information is collected to allow us to contact you regarding your submission and to help us understand more about the backgrounds and sectors of the people interested on our work.
- 5.69 We may publish the information you have shared in an anonymised form as part of our publication/summary of responses.

Do we share it with anyone?

- 5.70 We do not share personal details of our contributors with third parties. However, where we are working with a third party to carry out a consultation or where we need to verify information with a third party such as an accredited register, we may send the information in an anonymised form

Information regarding people who attend our events

What information we collect?

- 5.71 When you attend our events, we ask you to provide us with your name and contact details. We may be unable to confirm your attendance if you do not provide this. We may also ask you to provide your organisation name, job title, address and telephone number. This information is optional, and you do not have to provide it. However, providing this information will help us to identify future events that may be of interest to you.

Why we collect it?

- 5.72 This information is collected to allow us to produce an attendance list for the event that will assist people in networking and to facilitate communication with those attending (including the distribution of important information), both in advance of a meeting and afterwards (e.g. for the circulation of papers, the slides etc). This also allows us to support management and planning of events and to inform people of other future events that may be of interest.
- 5.73 We will also ask your consent to use your contact information to inform you about our research activity through our academic network. You may unsubscribe from this at any time by emailing info@professionalstandards.org.uk.
- 5.74 We also give people attending overnight at our academic conference the option of providing an emergency contact number and we may ask you for relevant health information such as food allergies for health and safety reasons.

Do we share it with anyone?

- 5.75 We will share your name with the venue the event is being held at to ensure security are aware of your presence for reasons of safety.
- 5.76 We may share information regarding food allergies with the venue to ensure this is catered for.

- 5.77 We will not share your details with any other third party without your express consent.

People who consent to being added to our mailing list

What information we collect?

- 5.78 When you respond positively to a request to receive communications from us, we ask you to provide us with your name, title and email address. We also ask you to provide your organisation name, type and geographical remit, job title, address and telephone number and information about areas of our work which are of interest to you. This additional information is optional, and you do not have to provide it.

Why we collect it?

- 5.79 This information is collected to allow us to send you regular updates about our work. It allows us to share information which is more relevant to your role and interests and helps us understand more about the backgrounds and sectors of the people interested on our work. You may unsubscribe from this at any time by emailing engagement@professionalstandards.org.uk.

Do we share it with anyone?

- 5.80 We will not share your details with third parties.

Information regarding fitness to practise cases

What information we collect?

- 5.81 We hold information about all final fitness to practise decisions taken by the Health and Social Care regulators and their Fitness to Practise Committees. The information that we hold includes information about the complaint, investigations of the complaint undertaken by the regulator (including evidence and witness statements); records of hearings; and records of the outcome of the complaint, including details of any formal findings and sanctions imposed (including warnings).
- 5.82 We may also hold information about professionals or patients, including medical records provided as part of a complaint as long as it is relevant to the investigation.

Why we collect it?

- 5.83 We collect this information in order to fulfil our responsibilities under section 29 of the NHS Reform and Health Care Professions Act 2002.
- 5.84 We review every final decision made by the fitness to practise committees of each health care regulator. If we decide that the decisions do not protect the public properly, we may refer them to the High Court or Court of Session in Scotland.

5.85 We may also use this information to create learning points letters that we share with the regulator.

Do we share it with anyone?

5.86 Most of the information is provided to us by the regulator. Each of the regulators have their own privacy statements regarding this information.

5.87 We may share this information with our external lawyers when reviewing the case and deciding whether or not to refer the case to Court. If the case is referred to Court we will share the relevant information with the Court.

5.88 Where we do not refer a case to Court we may send learning point letters to the regulator. Very occasionally, we may share information with other bodies such as the police or those with a responsibility for safeguarding, if we consider that disclosure is permitted by law and that it would be in the public interest to do so.

5.89 We may publish information relating to section 29 proceedings, including court judgments, consent orders and court orders, where publication is necessary to fulfil our statutory functions.

5.90 Published materials may remain available on the PSA website for an extended period and, in some cases, indefinitely, where continued publication is considered necessary and proportionate having regard to:

- Public protection
- Maintaining public confidence in professional regulation
- Informing the public about the PSA's exercise of its statutory functions
- The requirements of data protection legislation.

5.91 Before publication, the PSA considers whether:

- The registrant should be identifiable
- Personal data should be redacted
- Special category personal data should be redacted or anonymised
- Any court restrictions apply.

5.92 Publication decisions may be reviewed periodically and may be reconsidered following receipt of a request for removal, anonymisation or erasure.

5.93 We redact identifying details from case meeting notes where:

- The fitness to practise committee decided that the registrant's fitness to practise was not impaired, and that decision has not been overturned by the court/another fitness to practise committee
- The fitness to practise hearing was held in private

- The fitness to practise committee imposed a sanction that has an expiry date and the sanction has expired
- The fitness to practise committee found that the registrant's fitness to practise was impaired but did not impose a sanction – we redact the case meeting note after a six-month period.

- 5.94 Decisions regarding publication, redaction, anonymisation and retention are taken having regard to the PSA's statutory functions and obligations under data protection legislation.
- 5.95 Individuals who are identified in a court judgment, consent order or other published section 29 document may request that the PSA review whether continued publication of the information remains necessary.
- 5.96 Such requests will be assessed on an individual basis. The PSA will balance any impact on the individual against its statutory obligations and the public interest in publication.
- 5.97 We may occasionally allow researchers access to our database for the purposes of research in the public interest. All researchers are required to sign confidentiality agreements before access to the database is granted. Any published research will only contain anonymised data or personal information which is already in the public domain.

Performance review and Accredited Registers

What information do we collect?

- 5.98 As part of our performance review of the regulators and assessment of Accredited Registers we will look at a selection of cases that were closed at each stage of the fitness to practise / complaint process.
- 5.99 This information is assessed either at the regulators/registers premises or our offices. We have a secure file sharing system in place and we delete the information from our systems once we have completed the audit.
- 5.100 We may also consider information sent to us through 'share your experience' (see section on Complaint/share your experience information above).

Why we collect it?

- 5.101 We collect this information to check on how well the regulators and Accredited Registers have been protecting the public and promoting confidence in health and care professionals and themselves.

Do we share it with anyone?

- 5.102 Our performance review and accreditation assessment outcome reports are published on our website. We may discuss individual cases or complaints in our performance review reports, but if so we ensure that we don't provide information that allows identification of individuals involved.

Retention and disposal

- 5.103 The PSA sets out in detail its procedures for the retention and disposal of information and the timeframes for this to ensure that we carry this out consistently and that we document any actions taken.
- 5.104 Full details of how we do this can be found in our retention policy available on our website or on request from info@professionalstandards.org.uk

What are your rights

- 5.105 The PSA respects the rights of individuals to be in control of their own data. Subject to some legal exceptions you have the right to:
- The right to be informed
 - The right of access (subject access requests)
 - The right to rectification
 - The right to erasure
 - The right to restrict processing
 - The right to data portability
 - The right to object
 - Rights in relation to automated decision making and processing. .
- 5.106 We are fully committed to protecting your personal data and ensuring that we have appropriate technical and physical procedures in place and that our staff are trained in the relevant policies. If you have any questions about this or in relation to your rights, please contact Suzanne Dodds:

Suzanne Dodds
Professional Standards Authority
16-18, New Bridge St,
Blackfriars,
London,
EC4V 6AG

Or by email to suzanne.dodds@professionalstandards.org.uk

Your data abroad

- 5.107 The PSA does not currently process any personal data outside of the European Economic Area (EEA) unless the processing requires it (e.g. you have chosen to contact us using email or communications which route outside of the EEA).

- 5.108 In the unlikely event that the PSA does need to transfer or process data outside of the EEA we will make every effort to contact you and inform you of the reasons for this and of your rights.

Cookies

- 5.109 The PSA uses cookies from time to time to track traffic and help us to improve our user experience. For more information, please see our Cookie policy <https://www.professionalstandards.org.uk/cookie-policy>

Links to other sites

- 5.110 In order to improve your user, experience the PSA includes links to external sites (such as the Regulators) on our website. We are unable to control the privacy practices of these sites and therefore we strongly encourage you to read the privacy statement and understand how they collect information about you.

Appendix 1 – Explanation of lawful basis of processing

Lawful basis

Consent

Contract

Legal obligations

Vital Interests

Public task

Legitimate interests

Reason for processing

You have given us clear consent for to process your personal data for a specific purpose.

The processing is necessary for a contract we have with you, or because you have asked us to take specific steps before entering into a contract.

The processing is necessary for us to comply with the law (this excludes contractual obligations).

The processing is necessary to protect someone's life.

The processing is necessary for us to perform a task in the public interest or for our official functions, and this has a clear basis in law.

The processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply public authority processing data to perform our official role.)

Policy review

- 5.111 We will review these policies annually, or more frequently in the event of any legislative or regulatory changes.

Document Control

Version Control

Printed documents are uncontrolled. This document is only valid on the day it was printed.

Version	Description of Version	Date Completed
1.0	Combined policy documents for key internal and external facing documents i	June 2025
1.1	Reviewed and update the FOIA/DPA/ Individual rights policy with the new ICO contact details. Reviewed the information risk policy,	March 2026
1.2	Amendment to the Privacy notice to include monitoring office attendance	May 2026
1.3	Clarification of position and rights on publishing court judgements and consent orders	July 2026