

Employee Privacy Notice

Version 4.1 | August 2023

1 Purpose

This privacy notice is intended to give employees information about how PHSO uses and looks after information about you or that could identify you.

We manage this information in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679).

If you have any further queries, please email the Data Protection Officer dpo@ombudsman.org.uk

We are registered with the Information Commissioner's Office (ICO) as a Data Controller - registration number: Z6520944

Contact details for the PHSO DPO are:

Angharad Jackson

Data Protection Officer

Office of the Parliamentary and Health Service Ombudsman

PHSO CityGate

47-51 Mosley Street

Manchester

M2 3HQ

DPO@Ombudsman.org.uk

How your information will be used

- 1.1 PHSO asks you for information about you when you first start working for us and throughout your career with us. This is information required by the law or our contract with you. We do this so that we can pay you, train you, provide you with the right support and tools to do your job and make sure you can access employee benefits.
- 1.2 When you leave PHSO we will retain the information that the law or our contract with you says we need to keep.
- 1.3 PHSO is committed to the safe use and management of your personal data (information about you or that could identify you). We do this in compliance with the law including the General Data Protection Regulation (GDPR).

2 What information do we hold about you?

- 2.1 We create information to identify you for security purposes. Examples include photographic ID cards, network usernames and passwords and pre-employment checks.
- 2.2 We create information to identify you uniquely so that you can do your job and we can pay you. Examples include email addresses and payroll numbers.
- 2.3 We hold and use information about your health and wellbeing. Examples include filing fit notes for absences from work, details of disabilities and corresponding reasonable adjustments made, recording accidents in our accident book or sometimes personal confidences made in one-to-ones with your manager.
- 2.4 We ask all staff to provide us with current contact information in event of an emergency, serious incident, or systems failure. We test this regularly through SMS messaging. This emergency contact information is kept securely.
- 2.5 Most of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees.

- 2.6 We will ask for your consent before we use or record information relating to your racial or ethnic origin, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation. The only exceptions will be when consent is not required by law or the information is required to protect your health in an emergency.
- 2.7 An example of when we may not need to ask for consent is use of biometric information for security purposes. This is information that is you, such as your fingerprints, your DNA, your likeness (photographs), your signature and how you walk (gait analysis).
- 2.8 Biometrics are often used as the third level of security (see section 5 for details). Passwords are something you know (single factor), tokens like the ones we use for remote working are something you have (two factor) and finally biometrics which are something you are. This is one of the reasons why GDPR includes biometrics as part of a type of information about you that requires additional protection. However, your right to privacy is not outweighed by PHSO's need to secure the information we hold on behalf of complainants. Hence, we can ask you for your photograph as part of our arrangements to control who has access to our buildings and hence our information. This is when your consent is not required by law.
- 2.9 An example of when we will ask for your consent is if we want to take photographs of you at an event and use those in our communications. In these circumstances we must ask you for your consent as there is no legal obligation that overrides your privacy rights.
- 2.10 Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

3 Recording of training and learning events

- 3.1 As part of working at PHSO, we encourage and support all our colleagues to take part in training and continuous professional development. When you participate in a workshop or training event, we may choose to record the session. This is so we can make recordings or videos of sessions available to other members of staff who may not have been able to attend by uploading to our

in-house learning platform. As an attendee your image, voice or other participation such as chat comments, may be captured.

- 3.2 We will always let you know in advance if a session is being recorded and if you have any concerns, please raise it with the session organiser before the event so that they can make the relevant arrangements with you.
- 3.3 Recordings of training and learning events will only ever be available to an internal audience of your colleagues. We will not publish any recordings to the public internet, for example, such as on our website. Agreeing to recording does not impact on your information rights. This means that you can ask for copies of your personal information or for your personal information to be removed. It may be that we are unable to carry out your request and if so, we will write to you to let you know why. Recordings of training events will usually remain in our systems for 2 years from the recording date.

4 Personal information created through use of IT systems

- 4.1 Whenever you use PHSO's ICT systems or devices, it leaves a data footprint. Examples of this included timestamps of when you completed certain activities such as logging in or off the network, edited a document, completed a training course or logged a call to the HelpHub.

- 4.2 This information is personal in that it relates to, and identifies, you. Managers in PHSO can request this information with the exception of information gather via Nulia (see section 4). Their request will be approved only if a valid business reason is provided such as managing performance and must be approved by a senior manager. Access to this information is allowed under GDPR if it is necessary to manage our contract with you.
- 4.3 As this is personal information, you have the right of access to this data. You also have the right to ask us to put the information right if you believe it to be inaccurate (right to rectification), to delete the information (right to erasure), or the right to ask us to stop using this information (restrict processing). If you want to exercise these rights, then please contact informationrights@ombudsman.org.uk. Your request will be considered but please note, may not be accepted. If your request is rejected, you will be told why and how to appeal to the Information Commissioner's Office.

5 Information collected via your use of Microsoft

- 5.1 Everyone who works at PHSO uses Microsoft 365 (M365) to do their jobs. M365 is Microsoft online, the package of software, tools and solutions that power our work.
- 5.2 We write letters and papers in Word, share our ideas in PowerPoint, collaborate in Team and pool our knowledge in SharePoint. But not all of us know how to use these tools to our best advantage.
- 5.3 Nulia is a tool designed to help us work more effectively by providing tips and guidance at the right time. Nulia sits in the background observing how we work so that it can recommend personalised advice to each user. To do this, it needs to know the user and it does that by collecting and analysing data on each and every interaction.

- 5.4 As this is personal information, you have the right of access to this data. You also have the right to ask us to put the information right if you believe it to be inaccurate (right to rectification), to delete the information (right to erasure), or the right to ask us to stop using this information (restrict processing). If you want to exercise these rights, then please contact informationrights@ombudsman.org.uk. Your request will be considered but please note, may not be accepted. If your request is rejected, you will be told why and how to appeal to the Information Commissioner's Office.
- 5.5 For more information about information gathered via using Nulia, please see the detailed Annex A: Employee Privacy Notice Nulia

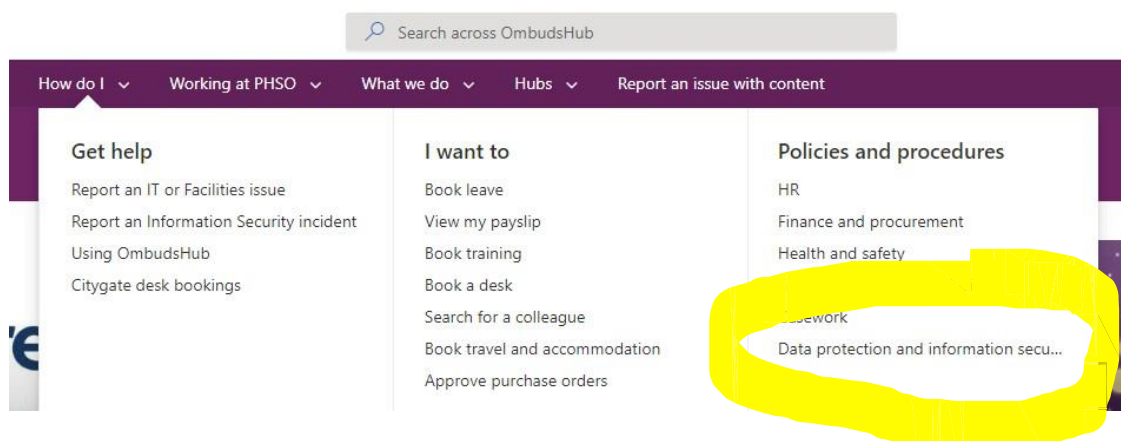
6 Biometric data

- 6.1 Biometrics are something you are as explained above. This makes biometric identifiers like fingerprints, iris prints and facial recognition very useful as part of a multi-factor approach to security. Multifactor is when we use two of more of the following to identify that you really are who you say you are when you log into PHSO's network or devices.
- Something you know (a password, a phrase, an answer to a question)
 - Something you have (a token, a device, a phone)
 - Something you are (fingerprint, voice stamp, face)

- 6.2 Using biometrics as part of a sign-in solution can be much more user friendly as there is nothing to remember. But because biometrics are ‘you’, then PHSO will take steps to ensure that it is kept securely.
- 6.3 PHSO undertakes to collect and use biometric data solely for the purposes of authentication to our systems, officers and information. This means that we will never use your personal biometric data for any other purpose or share this data with any other organisation unless required to do so by law.
- 6.4 PHSO will also only hold biometric identifiers for one calendar month after employees have left the organisation and will ensure that these are securely destroyed.

7 What do we expect from you?

- 7.1 It is your responsibility to update Human Resources, via HR Self Service or email HRSharedServices@ombudsman.org.uk with any changes to your emergency contact information.
- 7.2 We also expect that everyone who works for us will take care when handling information about other people including colleagues and complainants. For more information on this, please see our information and data protection library of policies, hints and tips on metacompliance <https://cloud.metacompliance.com/MyComplianceLibrary/MyComplianceLibraryIndex> which you can find via the How do I? menu on Ombudshub



- 7.3 To find out more about your information rights or if you want to find out more about how long you should be keeping, storing, saving or archiving information, contact the Information Rights Team at ++informationrights@ombudsman.org.uk
- 7.4 For security advice and guidance or to report any concerns you may have, please contact security via helphub

8 Who do we share your information with and why?

- 8.1 PHSO will only share information about you or that can identify you with other organisations if we are legally obliged to do so or to comply with our employment contract with you.
- 8.2 We will normally hold your information for six years. For a detailed breakdown, please refer to the [retention schedule for our HR records](#) available via [Metacompliance](#)
- 8.3 If in the future we intend to use information about or that can identify you differently, we will amend this privacy notice and inform anyone who may be involved. If necessary, we will ask for your consent.

9 What about my privacy at work?

- 9.1 You should assume that anything written or created using PHSO communications can be retrieved and viewed if necessary, for audit, management review or information security purposes. See section 3, 4 and Annex A for further information.
- 9.2 If you use PHSO systems for personal use, PHSO will record that activity.
- 9.3 This is detailed in our [Acceptable Use Policy](#) and if you have any queries or concerns, please contact the Data Protection Officer at DPO@ombudsman.org.uk

10 Your rights

- 10.1 You have rights under the General Data Protection Regulation (GDPR).

- 10.2 You have the right to be informed about how we use your information. This is called a privacy notice and you're reading an example
- 10.3 You have the right to request a copy of information we hold about you and this is free of charge.
- 10.4 We may however not be able to give you the information you are after if, for example, if it contains personal information about other people or if the information has been given to us in confidence.
- 10.5 You have the right to ask us to delete your personal data, also known as the right to be forgotten. If we agree to delete your personal data, we may still need to keep just enough information for us to record that we have completed your request. There are circumstances where we cannot agree to delete your data. This is when we are bound by law to keep information for longer such as pension or tax information.
- 10.6 You have the right to ask us to not use information about you or that identifies you for certain purposes. This is limited in practice given that PHSO only uses this information in accordance with the law or our contract with you. However, when appropriate we will try to accommodate your wishes or provide you with an explanation why we can't fulfil your request.
- 10.7 If we can fulfil your request, we will retain just enough information about you to make sure your wishes are respected in the future.
- 10.8 We will not sell your information or use it for commercial purposes.
- 10.9 If you would like a copy of some or all of the personal information we hold about you, you can ask your manager, Human Resources or contact the Information Rights team by writing to the address above or emailing: informationrights@ombudsman.org.uk

11 How to complain

- 11.1 If you are unhappy with how we have handled your personal information, please contact PHSO's Data Protection Officer DPO@Ombudsman.org.uk in the first instance. The DPO is Angharad Jackson.

11.2 You may also contact the Information Commissioner's Office.

The Information Commissioner
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF

Phone: 08456 30 60 60 Website: www.ico.gov.uk

12 Related documents

12.1 You may find the following documents useful.

13 Version control

Date	Version	Content/changes made	Owner of changes
25/5/2018	1		AJ
24/11/2020	2	Added ICT generated metadata	AJ
29/1/2021	3	Tweaks to language for accessibility	AJ
11/10/2022	4	Updated to reflect hybrid working, biometrics and Nulia	AJ
25/08/2023	4.1	Learning and Development update	AD