WASPI PRIVACY NOTICE

WHY WE USE PERSONAL DATA

The Wales Accord on the Sharing of Personal Information (WASPI) is supported by the Welsh Government, and hosted by Digital Health and Care Wales (DHCW), as the 'single' information sharing framework for Wales. The purpose of the framework is to enable service-providing organisations to share relevant personal information in a lawful and safe way, therefore supporting risk management. In particular, it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others. For further information on WASPI, please see: https://www.waspi.gov.wales/

DHCW is a Special Health Authority, part of the NHS Wales family and a trusted partner, DHCW is taking forward the next generation of services needed to transform health and care delivery. As the host of the WASPI Service, the information held by WASPI is hosted on DHCW's infrastructure. For further information on DHCW, please see: https://dhcw.nhs.wales/

As part of WASPI, we may use personal data for the following purposes:

- **Accord Sign-Up:** Where individuals have signed up to the Accord as the designated officer for their organisation, we will retain a record of the details provided on their registration and they may be contacted in relation to WASPI services.
- **Information Sharing Agreement Development (including Regional Quality Assurance Groups):** Where individuals have created an Information Sharing Agreement using any of the WASPI branded templates and engaged with the WASPI team (including use of WASPI Information Sharing Protocol template through the Regional Quality Assurance Groups), WASPI will hold information provided as part of the agreement and any supplementary information in relation to the service, project or initiative the agreement supports.
- **Newsletter:** Where individuals have opted-in to receiving the WASPI newsletter, they will be contacted to receive a newsletter relating to WASPI services. Recipients of the WASPI newsletter can contact the WASPI service at any time to opt-out of receiving the newsletter.
- **Information Sharing Gateway (ISG):** The ISG has been developed by a sub-group of organisations in the Lancashire & Cumbria IG Group in order to improve and modernise the administration and risk assessment of information sharing in the public sector. It has been designed by IG specialists, for IG specialists, to support their IG reporting on data flows and information sharing. The data sharing functionality within the system includes digitised versions of WASPI information sharing agreement templates. Information provided will be used solely for the purpose of registration to the system.
- **Events and Training:** Information provided in relation to events and training that WASPI hosts, participates in or attends may be used by the WASPI Service for the purpose of: planning and organising the relevant event following registration; future planning (such as where feedback is provided); or promotional purposes (such as photos and videos –

subject to the relevant notices informing individuals of photography and filming and providing the option to opt-out of this).

- **Contacting the Team:** Where individuals contact the service for queries, questions or advice, WASPI will hold the information provided relevant to the correspondence.

Access to this data is controlled. Generally, access will only be by the WASPI service and only where required. We only allow access to personal data where it is required for somebody to do their job. DHCW and WASPI take this seriously and all of our employees are required to be trained on the appropriate use of personal data. Inappropriate access to personal data can result in disciplinary action, including dismissal.

For further information about DHCW's establishment and functions, please see: Digital Health and Care Wales: establishment and functions | GOV.WALES

TYPES OF PERSONAL DATA

To maintain the WASPI framework, we collect, store and use limited personal data ('processing').

We do not collect or process all of this personal data about all people all of the time. We only collect and process the personal data necessary for the particular task that we are carrying out. Where possible, information about you will be pseudonymised (replacing identifiers with codes or 'keys') or anonymised (meaning individuals cannot be identified); for example, when reports are produced.

The categories of personal data we process include:

- Basic demographic information, such as name and job role,
- Contact information such, as email address and phone number,
- Information you provide relevant to meeting your needs at events or training we host, such as dietary or accessibility requirements,
- Images or photographs of you at events or training that we host, participate in or attend.

Please note WASPI does not store any information about service users involved in the information sharing agreements produced, where DHCW is not a partner to the agreement.

HOW WE USE PERSONAL DATA

Personal data is required for the maintenance of the WASPI framework as set out above.

HOW WE OBTAIN PERSONAL DATA

The personal data held will generally be provided by you. On occasion this may be provided by another person, such as where you are listed as being a partner organisation or consulted on in an information sharing agreement.

THE LAWFUL BASIS FOR WHAT WE DO

Data protection legislation requires us to tell you the lawful basis for processing personal data in the way we do. Further information is available from the website of the Information Commissioner's Office. Click here for more information.

We rely on the following legal provisions:

- Public task: the processing is necessary to perform a task in the public interest.
- Legitimate interests.
- Where deemed appropriate, we may ask permission to use personal data about you.

WHO PERSONAL DATA IS SHARED WITH

Personal data is only shared with other organisations where it is necessary and lawful to do so.

We may share your personal information with the following organisations in these specific scenarios:

ISG: To maintain the system and provide access.

Regional Quality Assurance Groups: Where an Information Sharing Protocol has been submitted.

We will share personal data if we are required to do so by law – for example, by court order or to prevent fraud or other crimes.

We may use 'cloud' services, which means personal data may be stored outside of the European Economic Area. If this occurs, we are obliged to have in place appropriate safeguards implemented with a view to protecting data in accordance with applicable laws. Please use the contact details below if you want more information about the safeguards that are currently in place.

Anyone receiving personal data about you is under a legal duty to keep it confidential. We only request, use and share the minimum personal data necessary. We will never sell personal data about you, and we will not share it without the appropriate legal authority, or if appropriate to the circumstances, your informed consent.

HOW LONG WE KEEP PERSONAL DATA

We keep personal data for as long as we need to in order to fulfil the purpose(s) for which it was collected and to comply with our legal and regulatory obligations.

SECURITY AND STORAGE OF DATA

DHCW recognises that personal data is very valuable and so we take its security very seriously. We have set up systems and processes to prevent unauthorised access or disclosure of data through the use of:

- Auditing - we keep records of those who access personal data;
- Password controls - members of staff are provided with their own username and password to access personal data;
- Access controls – only those staff that are required to access the data have access to the data;
- Electronic records management - all data is stored confidentially and in secure locations;
- Computer controls - we have complex security controls to ensure our computers cannot be accessed by those not authorised to do so – such as hackers;
- Storage – We have sophisticated storage solutions with back up for resiliency; and
- Encryption - computer devices that hold personal data such as laptops are encrypted in case the device storing the data is lost or stolen.

All DHCW staff must complete Information Governance training. This training makes staff aware of the importance of the confidentiality and security of personal data and makes clear that they are personally responsible for the security of such data. This training must be completed every two years.

We also make sure that any third parties we deal with keep all personal data they process on our behalf safe and secure.

YOUR RIGHTS

Data Protection legislation provides various individual rights for data subjects including:

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Not all of these rights are absolute, which means we often have to balance your wishes against other requirements. This is because there are other legal reasons that such records need to be kept. Each request to exercise one of the above rights will be assessed on its merits. Some rights are unlikely to apply in the context of the work we do; for example, the right to erasure and right to portability.

For an explanation of all your rights please see the ICO's guidance, which you can access here.

If you wish to exercise any of these rights or have any queries or concerns regarding our processing of personal data about you, please contact us using the contact details provided below.

CHANGES TO THIS POLICY

We keep our privacy notice under regular review to ensure it remains relevant, accurate and up to date. Any changes to this privacy notice will apply to you and the information held about you immediately.

CONTACT US

Please contact DHCW's Data Protection Officer for further information regarding this policy, including how to exercise your rights:

Data Protection Officer
Digital Health and Care Wales
Tŷ Glan-yr-Afon
21 Cowbridge Road East
Cardiff
CF11 9AD

DHCW.InformationGovernance@wales.nhs.uk

RIGHT OF COMPLAINT

You have the right to lodge a complaint in relation to this privacy notice or our processing activities with the Information Commissioner's Office, which you can do through the website or their telephone helpline.

https://ico.org.uk/global/contact-us/

DEFINITIONS

Term	Definition
Data Protection Officer	Certain categories of organisation, including any public body or authority (except courts in their judicial capacity) are required to designate a suitably qualified Data Protection Officer (DPO). The tasks of the DPO are set out in Article 39 of UK GDPR
Data subject	A 'data subject' is an identified or identifiable natural person.
Data Protection Legislation	The UK GDPR is the retained EU law version of the EU's General Data Protection Regulation (GDPR). It contains the definitions, conditions, principles and rights that apply to the processing of personal data in the UK. The Data Protection Act 2018 creates specific provisions, such as exemptions allowed by UK GDPR, and incorporates

	the provisions of EU Data Protection Directive 2016/680 – the Law Enforcement Directive.
Personal data	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
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
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
Pseudonymised data / Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Last updated: September 2025