Code of **Conduct**

CONTENTS

The Wales Accord on the Sharing of Personal Information (WASPI) is an existing good practice measure. This code focuses on specific risks identified over years of WASPI implementation. The code provides members and their stakeholders with additional assurances that their information sharing practices are compliant with data protection legislation and are following good practice.

The code is not intended as a barrier to the sharing of personal data and should not be used as such. The sharing of personal data can be lawful and appropriate without code membership. The rights and freedoms of individuals must be the primary concern of all WASPI stakeholders.

Adherence to this code does not mean that a code member is compliant with the whole UK General Data Protection Regulation, only to the elements that fall within the scope of the code.

Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information

Section 1 – Definitions

In this code:

ICO means the Information Commissioner's Office.

Data Protection legislation means all applicable laws, regulations and regulatory rules which govern the processing of personal data including (i) the Data Protection Act 2018, Regulation (EU) 2016/679 the General Data Protection Regulation as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and any subsequent legislation enacted and duly in force from time to time relating to the processing of Personal Data; and (ii) all guidance and / or codes of practice issued from time to time by the Information Commissioner or relevant government department, and any relevant rulings from time to time of the Information Commissioner or of the Courts of England and Wales relating to the processing of Personal Data.

Personal Data, Data Subject and **Processor** have the meanings given in the Data Protection Legislation.

ICO Code of Conduct means voluntary accountability tools, enabling sectors to identify and resolve key data protection challenges in their sector with assurance from ICO that the code, and its monitoring, is appropriate as defined by the ICO.

WASPI means the Wales Accord on the Sharing of Personal Information. A good practice framework, which allows organisations directly concerned with health, education, safety, crime prevention and social well being of people in Wales to share information effectively, safely and lawfully in line with the ICO's Data Sharing Code of Practice.

ISP means Information Sharing Protocol. A data sharing agreement which supports the regular and reciprocal sharing of personal information between data controllers for a specified purpose. A template ISP document is maintained and held by WASPI. Any ISPs produced on the WASPI ISP template must follow the WASPI Quality Assurance process.

Quality Assurance Process is the process through which Information Sharing Protocols are checked for consistent use of the WASPI templates and appropriate application of the data protection legislation. The process involves five regional Quality Assurance groups across Wales overseeing the process.

WASPI Accord is a common set of principles and standards which support the sharing of personal information to deliver services to the people of Wales. Signing the Accord allows an organisation to become a "WASPI member" and demonstrates a commitment to apply the principles within the Code. WASPI membership is separate to Code Membership and is therefore not detailed within this Code. However, organisations looking to attain Code Membership are encouraged to sign up to the Accord before submitting their application. Further detail on WASPI membership can be found via the WASPI website.

Monitoring Body means a legal entity, or a defined part of a legal entity such that it is legally responsible for its monitoring activities. The monitoring body shall agree to be responsible for its monitoring role and therefore responsible for a fine under UK GDPR Article 83(4)(c) and S.155 DPA 2018.

Code Owner means associations or other bodies representing categories of controllers or processors who have responsibility of the code, ensures the code is periodically reviewed, and that capacity and tools are provided to the monitoring body to discharge their responsibilities.

DHCW means Digital Health and Care Wales. A Special Health Authority and statutory body established under statutory instrument 2020 No. 1451 (W.313), 'The Digital Health and Care Wales (Establishment and Membership) Order 2020'.

Section 2 – Overview

- Article 40 of the UK GDPR makes provision for the preparation of codes of conduct to help organisations apply the legislation in practice.
- This code supports the sharing of personal data, between members and other stakeholders, for the purposes of providing services that – directly or indirectly –support or promote the health, wellbeing, education, security and safety of citizens in Wales. It applies to controllers as defined by data protection legislation.
- The aim of this code is to build upon the existing Wales Accord on the Sharing of Personal Information (WASPI) framework to address key risks that threaten organisational compliance with the WASPI principles and the effective and lawful sharing of personal data. Codifying requirements offers code members and their stakeholders – including the public – additional assurance around organisational practices of data sharing. **This code is an expansion of the WASPI Accord, not a replacement.**
    - This code is focused on specific risks relevant to sharing of personal data for the above purposes and builds upon the existing commitments that the WASPI framework provides.
    - The code provides an additional level of assurance for organisations that regularly share high volumes of personal data, and/or special categories of data, with multiple stakeholders through its formal monitoring body arrangements.
    - The WASPI framework is committed to supporting all organisations with the effective sharing of personal information. To ensure that the framework continues to support all organisations, the framework templates will continue to be actively available for all organisations signed up to the WASPI principles and acceptance of the Accord. Compliance with code membership as set out within this code, will offer the additional benefits and compliance to organisations.

- Organisations that would benefit from the additional level of assurance provided by the code can apply for code membership. Acceptance is subject to the provision of appropriate evidence that demonstrates an organisation can meet the pre-requisites set out in the application procedure. Organisations accepted as code members will be bound by the terms of the code for as long as they remain members.
- Code membership will provide additional assurances for organisations that regularly share high volumes of personal data, and/or special categories of data, with multiple stakeholders and provide increased public trust and confidence in respect of personal information data sharing.

- Adherence to this code does not mean that a code member is compliant with the whole UK GDPR, only to the elements that fall within the scope of the code. Code membership, and the associated monitoring of requirements, provides assurance and confidence to organisations, their stakeholders and the public that information sharing practices are compliant with legislative requirements.
- The first iteration of the code is being provided within the current WASPI funding model. There will be no cost to code members, but this may be revisited if the requirements of the code and/or the associated services change. Any proposal to charge for code membership will be subject to consultation with the WASPI Management Advisory Board and all stakeholders. Code members will be under no obligation to continue membership if a funded model is introduced at a later date.

Section 3 – Background

Sharing personal data is an essential element of delivering effective services to citizens.

The existing **Wales Accord on the Sharing of Personal Information (WASPI)** is a framework for those organisations that hold information about individuals (personal data) and who consider it appropriate or necessary to share it with others.

WASPI is a voluntary framework that has been available for over a decade. It was established to address challenges faced by stakeholders who needed to share the personal data of citizens to offer care, treatment, support, education and protection. The various iterations of the Accord have drawn on the legislation and available guidance, such as the Information Commissioner's Data Sharing Code of Practice, to introduce a set of principles that signatories agree to apply when sharing personal data.

Wide support for WASPI has helped organisations from different sectors to adopt a consistent approach to sharing personal data. This in turn helped build confidence that personal data can, and should, be shared to deliver services that benefit people in Wales. The development of standardised templates for information sharing agreements, with an associated quality assurance process, underpins the principles set out in the Accord and has helped organisations to demonstrate how their information sharing arrangements are lawful and appropriate. Sharing good practice is a fundamental aim of WASPI and an open library of over 200 quality assured Information Sharing Protocols is available on a bespoke website. WASPI has extensive support, including public statements of support from the Information Commissioner and Welsh Government.

As of September 2022, over 750 organisations were signatories to existing WASPI Accord, including:

All Welsh Health Boards and Trusts

All Welsh Local Authorities

All Welsh Police Forces and associated Police and Crime Commissioners

All Welsh Fire and Rescue Services

Welsh Government and the Welsh Parliament

The National Probation Service (Wales)

Education providers (schools, colleges, early years providers and others)

General Medical Practices

Community Health Councils

Housing Associations

Voluntary sectors organisations and charities

And a range of other partners including Transport for Wales, Careers Wales and the Welsh Local Government Association.

Digital Health and Care Wales (DHCW) is a Special Health Authority and statutory body established under statutory instrument 2020 No. 1451 (W.313), 'The Digital Health and Care Wales (Establishment and Membership) Order 2020'. DHCW and its preceding organisation, NHS Wales Informatics Service (NWIS), have provided a central support function for WASPI since 2010, with funding for this service incorporated into DHCW's core financial model. A sub-team of DHCW's Information Governance Team provides the support required to maintain and develop WASPI. Duties and responsibilities include:

- Administrative and secretariat support for the for the five regional quality assurance groups, including an initial check of all submitted ISPs.
- Secretariat and management of the WASPI Management Advisory Board.
- Reviewing and updating the Accord and associated framework documentation including data sharing templates.
- Maintenance and development of a bespoke WASPI website.
- Promotion of WASPI with stakeholders.

As the owners of the WASPI framework and with extensive experience of maintaining and developing WASPI, representing and liaising with stakeholders to promote the framework, DHCW is considered an appropriate code owner. The WASPI Team, within DHCW's Information Governance Team, will be the monitoring body for the purposes of the code. Its staff are experienced in administering WASPI, are qualified in information rights legislation and supported by DHCW to obtain professional membership, where appropriate.

The WASPI Team is funded through Welsh Government and resides within DHCW. The team are able to demonstrate independence from DHCW in this regard, as any decisions made shall not be subject to approval by DHCW or any other organisation. Further information is provided in section 8 of this code.

Section 4 – Consultation

A Consultation and Communication Strategy has been developed and once initial triage assessment of the code has been sought through the ICO Regulatory Assurance Department, this consultation process will undertake an extensive programme of formal stakeholder and public consultation. The feedback from this will be published and will be used to strengthen the final application to be submitted to the ICO for this Code of Conduct. This is set out in Appendix F.

Section 5 - Compliance with national legislation

This code promotes compliance with national legislation, namely the UK GDPR. Although part 3 of the Data Protection Act 2018 (DPA 2018) contains no equivalent of Article 40 of the UK GDPR, the principles of UK GDPR and the DPA 2018 are closely aligned. Most organisations processing personal data for the "law enforcement purposes" (as defined by data protection legislation) also process data for non-law enforcement purposes and information sharing agreements developed using WASPI often include a combination of lawful bases from UK GDPR and DPA 2018. As such, code membership raises the standards of existing data sharing principles and templates provided by WASPI and seeks to provide assurances above the standards of the UK GDPR on around data sharing. This in turn, provides benefits to all organisations processing personal data allowing better delivery of services for the benefit of citizens.

The code does not replace or contradict any other national legislation which applies to the sharing of personal data. The code supports organisations with ensuring they have documented mechanisms to set out lawful basis of data sharing which will relate to applicable cross sectoral national legislation and can assist organisations with mitigating against risks of potential data breaches.

The code promotes assurances for organisations and the public, that data sharing between partner organisations is lawful, as well as providing an effective review mechanism.

Code members will need to undertake their own assessment of the compatibility of information sharing initiatives with relevant legislation and common law, such as the common law duty of confidentiality.

Neither the code, nor any of the associated standard templates replaces the need for a contract or agreement with a processor or an arrangement setting out Joint Controller responsibilities, as required by data protection legislation. These requirements are outside the scope of this code.

Section 6 – About this code and the benefits

BENEFITS OF THE CODE

Providing standardised documentation and an established governance framework, WASPI helps service-providing organisations to share relevant personal information safely and lawfully.

The code ensures consistent application of principles for sharing of data, ensures relevant agreements are reviewed and updated and ensures good governance and accountability aligned to the ICO data sharing code of practice.

The code provides an approved assurance model for organisations to confidently document the lawful sharing of personal and sensitive data across multiple sectors.

THE CODE

This code seeks to be approved by the Information Commissioner's Office under the provisions of article 40 of the UK General Data Protection Regulation (UK GDPR). **It does not replace WASPI;** the Accord, WASPI templates and guidance, remain relevant to all organisations who need to share personal data to provide effective services to people in Wales.

The code introduces approaches to data sharing which accounts for the respective needs of all organisations.

WHO IS THE CODE FOR?

Any organisation that needs to share personal data to deliver services aimed at the health, wellbeing, education, security and safeguarding of citizens in Wales, when considering whether code membership is for them, organisations should consider:

- The scale of personal data they process.
- The risk profile of that data.
- The number of employees with access to personal data.
- The frequency of information sharing.

WHAT IS THE CODE TRYING TO ACHIEVE?

1. Addressing key risks to effective and lawful information sharing of personal data by: **Reinforcing** WASPI as the information sharing framework in Wales.
2. Ensuring the **consistent application of WASPI principles** through an emphasis on the importance of the quality assurance processes.
3. **Maintaining the relevance of agreements** by insisting they are regularly reviewed and updated.
4. Encouraging code members to demonstrate good **governance and accountability**.

The code intends to add additional value to organisations by identifying requirements and monitoring mechanisms that address specific elements of good practice and focus on identified risks to the lawful and effective sharing of personal data. The code's requirements reflect guidance and recommendations from the ICO – for example elements of its **Accountability Framework and data sharing code of practice** – and seek to address areas where we know, from experience, improvements can be made.

Code members are subject to monitoring and potential sanctions for non-compliance with the code's requirements. These assurance measures are where the code adds most value, by holding members to a higher standard of practice. In return, code members will be able to evidence that they have met the requirements and achieved code membership by **displaying a code of conduct WASPI badge** as detailed below.

WASPI CODE OF CONDUCT MEMBER BADGE

AELOD COD YMDDYGIAD
CODE OF CONDUCT MEMBER
Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information

This badge will be provided by the monitoring body to each code member once code membership has been confirmed and is for the code member to display as long as an organisation remains a code member. If code membership is removed or withdrawn, the monitoring body will inform the organisation to no longer use the code of conduct badge.

The code provides particular focus for organisations to be able to demonstrate compliance with the UK GDPR Article 5 obligations.

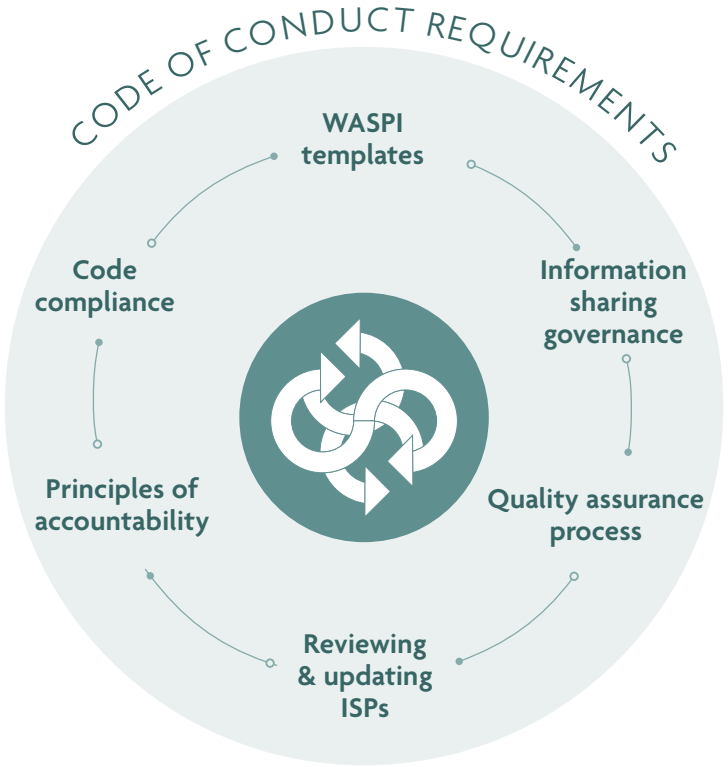
Code members, by meeting and continually demonstrating the requirements of code membership will be meeting standards expected of the ICO based on they accountability framework and tracker, specifically in demonstrating how compliance is being achieved against direction and support, awareness and training, transparency and lawful basis for processing.

The Information Sharing Protocol puts into practice, the ICO's data sharing code of practice, which states that it is good practice to have an information/data sharing agreements which sets out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities. Having an agreement in place helps organisations to demonstrate that they are meeting your accountability obligations under the UK GDPR.

6.1 WASPI CODE OF CONDUCT REQUIREMENTS

There are six areas of requirements that any code member will need to demonstrate compliance against. Evidence of compliance against each area will be assessed through ongoing commitment to processes of quality assurance, evidence provided by code members through their annual assurance and more thoroughly as part of in-depth audits cycles, committed within the WASPI code of conduct Audit Strategy and as detailed within the monitoring mechanisms.

Further details of each of these requirements and how the monitoring body will monitor a code member are set out within section 7.



6.2 EXAMPLES OF RISKS AND MITIGATION PROVIDED BY THE CODE

AGREEMENTS		
Risk description	**Example**	**How the code mitigates the risk**
If... Code Members use alternative data sharing templates or do not document their data sharing activities. **Then...** the consistent approach developed over many years in Wales will be threatened or organisations compliance with accountability and transparency requirements will not be met. **Resulting in...** a return to a fragmented approach to the development of Information Sharing Protocols, which could delay the sharing of personal information or result in non-compliant practices or no documented data sharing taken place. This could have a negative impact on the rights and freedoms of individuals who may not receive the services they need or may see their privacy impinged or result in organisations being non-compliant with the data controller obligations.	A public authority commissioning a third party to draft an information sharing agreement aimed at sharing information between health and social care for the purposes of delivering a range of services to citizens. The agreement was circulated to other stakeholders, who, declined to use it.	By signing up to the code, members of the code would be using a committed set of templates to document the sharing of personal data. This would significantly reduce risks of organisations using fragmented approaches and through the assurance controls and monitoring mechanisms enable organisations to have assurance of sharing agreements which would be regularly reviewed. Use of templates under the Code will enable organisations to document data sharing activities in a consistent manner and provide citizens with details of how data sharing is compliant with a data controllers obligations with Article 5 (1)(a) of the UK GDPR.

QUALITY ASSURANCE		
Risk description	**Example**	**How the code mitigates the risk**
If... signatories to the code by-pass or do not engage with the agreed quality assurance process. **Then...** the integrity of data sharing processes and code will be affected with an associated deterioration in the quality of Information Sharing Protocols. **Resulting in...** the potential for non-compliance with data protection legislation and recognised good practice, with the risk of inappropriate sharing that leads to challenges by citizens and/or regulators. Again, this risks delays to services or impingement of individuals' privacy.	A public sector organisation does not regularly attend the relevant, regional quality assurance group. An Information Sharing Protocol is assured by the group but the organisation in question, later challenges the content and causes delay in the agreement being signed by the partner organisations. This forced other partners to run at risk (i.e. to share personal data without an agreement) or to delay the provision of the service. This could have been avoided if the organisation in question had engaged from the outset.	The five quality assurance groups across Wales are key to the continuation of WASPI. They operate on a voluntary basis and are stakeholder led, with an emphasis on large public sector bodies to maintain them. Code members will be required to contribute to these group and to engage with the quality assurance process. This will help with an equitable distribution of responsibilities and engage tangible sanctions for members who do not follow agreed quality assurance processes and procedures.

REVIEWING AND UPDATING		
Risk description	**Example**	**How the code mitigates the risk**
If... agreements are not regularly reviewed and updated. **Then...** they may fail to account for changes in legislation, policy, good practice and service provision. **Resulting in...** outdated agreements that do not reflect practice and, as such, are non-compliant with data protection legislation. This will put organisations at risk, undermining stakeholder and public confidence, which could affect the willingness to share personal data or challenges to practice.	Over 250 Information Sharing Protocols have been quality assured and published as examples of good practice using WASPI processes. Whilst organisations use documented Information Sharing Protocols, they are not always regularly reviewed or updated. In many cases data sharing activities may have changed. For example, partner organisations who form part of the sharing arrangements, secure methods in which data is shared often change over a two-year cycle, and in some cases national legislation relied upon for data sharing is updated.	Code members will be required to regularly review ISPs to ensure they account for changes to legislation, policy, good practice and service provision. This will be monitored through monitoring body mechanisms. This assurance process will improve organisational practices and compliance as well as providing greater stakeholder confidence.

GOVERNANCE AND ACCOUNTABILITY		
Risk description	**Example**	**How the code mitigates the risk**
(i) **If...** organisations do not know what personal data they share, and with whom. **Then...** they are unable to ensure arrangements are lawful and appropriate. **Resulting in...** an inability to demonstrate good governance and accountability.	(i) WASPI publish a central register of Information Sharing Protocols to the WASPI website, which involve code members. This is not designed to replace information asset management at organisational level. Only WASPI Information Sharing Protocols are recorded on the register. Anecdotal evidence suggests that some organisations struggle to keep records of sharing agreements.	As part of their application for code membership, organisations will need to describe the accountability measures they have in place to underpin lawful and appropriate sharing of personal data. All Information Sharing Protocols for code members will be published on the WASPI website. This will provide code members with the ability to sign post individuals through privacy notices or queries to documented information sharing practices involving their organisation linked into their article 30 UK GDPR obligations and improving transparency.

continued on next page

GOVERNANCE AND ACCOUNTABILITY (Cont)		
Risk description	**Example**	**How the code mitigates the risk**
(ii) **If...** organisational structures do not facilitate accountability by ensuring that there are clear roles and responsibilities around the sharing of personal data, supported by clear reporting lines and routes of escalation. **Then...** there is a risk that the sharing of personal data becomes siloed in data protection or Information Governance teams without appropriate oversight. **Resulting in...** isolated pockets of good practice and a lack of coherent, organisational strategy that could impact on the rights and freedoms of data subjects.	(ii) Stakeholders reporting difficulties in obtaining signatures from all parties to information sharing agreements. This undermines the efforts that go into developing and quality assuring agreements. Without this final step, organisations cannot demonstrate that the sharing of personal data has received organisational approval.	Code members will be required to ensure that Information Sharing Protocols, their organisations are signed up to, are appropriately signed off. Monitoring and review mechanisms required by being a code member will enable consistent reviews of arrangements and provide additional forms of audit and assurance controls. This will allow code members to demonstrate compliance and provide increased public confidence in data sharing activities.

Section 7 - Requirements and monitoring mechanisms

The following requirements are intended to provide mitigation to the risks identified in section 6.2 of the code. Requirements need to add value by being specific and achievable. This code enhances processes and procedures developed under the WASPI framework and provides assurance controls, which will allow organisations signed up as code members to be able to demonstrate compliance towards their data protection compliance.

All requirements under this section are mandatory requirements for Code Members to adhere to. Non-compliance with these requirements may lead to the monitoring body carrying out its duties under section 11 of this code.

7.1 USING WASPI TEMPLATES

Consistency of approach is a core element of the WASPI framework. Its standardised templates have been developed over a number of years by data protection and information governance specialists. The consistent use of core templates builds confidence in the WASPI brand, which in turn provides assurance to stakeholders. It also enables a continuous development cycle where templates are implemented, tested in practice, reviewed and changed, where required.

This code focuses specifically on the Information Sharing Protocol template provided under the WASPI framework and its Quality Assurance process that is in place, which is supported by the five regional quality assurance groups.

RQ1 – WASPI CODE MEMBERS MUST USE STANDARD WASPI TEMPLATES RELEVANT TO THE RECIPROCAL SHARING OF PERSONAL DATA. (PT 1)	
Detail	**RQ1**(i) All WASPI code members will use the WASPI Information Sharing Protocol (ISP) template to document controller to controller, reciprocal sharing of personal data with other organisations that regularly design and/or deliver collaborative services to citizens in Wales. The ISP code member developing an ISP will: • Have overall responsibility for ISPs within their respective organisations and must therefore ensure ISPs are disseminated, understood and acted upon by relevant practitioners. • Regularly monitor and review the use of ISPs to ensure information is shared effectively and appropriately. • Ensure their respective organisations have appropriate privacy notices/disclaimers in place regarding the data sharing activities. • Prior to sharing personal information, respective organisations have considered or reviewed the need for and, where required, completed a Data Protection Impact Assessment to assess the legality, benefits and risks of data sharing.
Caveats	ISPs do not replace the need for data processing agreements / contracts where a third party data processor processes personal data on behalf of a controller or the arrangement required under data protection legislation setting out the responsibilities of joint controllers are sharing personal information. WASPI is designed to support services that provide or enable care, treatment, support, education or protection to be provided to citizens. WASPI templates are not designed to support sharing of data sets for analysis, planning or research.

continued on next page

Monitoring mechanism	- Application form. - The pre-quality assurance check performed by the Monitoring Body in line with the agreed quality assurance process. - The quality assurance of an ISP is undertaken by regional quality assurance groups. During this assurance process service leads with knowledge of the data sharing activities present the ISP. This helps to provide assurances on the data processing activities set out within and tests the application of the content of the ISP. Evidence and confirmation is required as part of this process to ensure that appropriate privacy notices and lawful basis for processing are met. Further evidence will be required to be submitted as part of annual assurance and audit processes. - Complaints / reports that code members are using non-WASPI templates. - A log of ISPs will be maintained.
Responsible body	- The Monitoring Body. - The Monitoring Body and Quality Assurance Groups will identify deviation. - Complaints / reports of non-compliance can be submitted to the Monitoring Body by any individual / organisation using the contact details on the WASPI website. - The Monitoring body will investigate in line with agreed procedures.

RQ1 – WASPI CODE MEMBERS MUST USE STANDARD WASPI TEMPLATES RELEVANT TO THE RECIPROCAL SHARING OF PERSONAL DATA. (PT 2)	
Detail	WASPI code members will not alter agreed templates without following due process; by either raising proposed changes with the WASPI Team or the relevant Quality Assurance Group in the first instance. Permanent changes to WASPI templates require final approval from the WASPI Management Advisory Board.
Caveats	Data controllers may make changes to the template in limited circumstances where agreed with regional ISP group members, however this will be only for limited purposes and will be agreed by all partners involved.
Monitoring mechanism	-The pre-quality assurance check in line with the agreed quality assurance process. -The quality assurance undertaken by regional groups and attended by the Monitoring Body.
Responsible body	-The Monitoring body and Regional Quality Assurance Groups will identify deviation. -Complaints / reports of non-compliance can be submitted by any individual / organisation using the contact details on the WASPI website. -The Monitoring Body will investigate in line with agreed procedures.

7.2 INFORMATION SHARING GOVERNANCE

Information sharing governance is key to allowing code members to demonstrate governance controls in place within their organisation which align to the code.

RQ2 – INFORMATION SHARING GOVERNANCE MUST ADDRESS DATA SUBJECT ACCESS RIGHTS, RECORDS MANAGEMENT AND DATA SECURITY FOR SHARING	
Detail	**RQ2**(i) All code members must set out governance accountability to ensure that an ISP meets requirements for assurance. This includes: • Have in place policies and procedures to uphold the confidentiality, integrity and availability of personal information with specific reference to the retention, storage and disposal of records. • Ensure that access to information requests for the information referenced in an ISP will be dealt with in accordance with the code members relevant policies and procedures. • Have an appropriate and adequate security framework for the sharing of personal information as set out within an ISP.
Caveats	None.
Monitoring mechanism	Monitoring Body in the quality assurance process, and through the annual assurance and audit processes
Responsible body	Monitoring Body in the quality assurance process (initial check, and attendance at meetings), and through the annual assurance and audit processes.

7.3 THE QUALITY ASSURANCE PROCESS

The quality assurance process is a core element of the WASPI framework, as it maintains the integrity of the standard templates and has helped to develop local and regional communities of practice.

RQ3 – A COMMITMENT TO THE QUALITY ASSURANCE PROCESS. (PT 1)	
Detail	**RQ3**(i) All code members must follow the agreed quality assured process, details of which are at Appendix B. This involves: • Submitting ISPs for quality assurance via the monitoring body. • Considering initial comments provided by the monitoring body and to determine if ISPs need to be amended prior to formal quality assurance. • Presenting ISPs at meetings or arranging for service leads to be present at meetings (where an organisation is the author / lead). • Ensuring amendments required by the respective QA group are actioned. • Ensuring finalised agreements are signed by an appropriate individual.
Caveats	None
Monitoring mechanism	In addition to the quality assurance procedure, Terms of Reference for the regional quality assurance groups will set expectations for code member engagement and attendance. These shall take into account factors such as the resources available to code members and the extent to which they are involved in complex data sharing.
Responsible body	Any code member must escalate instances of deviation from the agreed procedure and process – including approved Terms of Reference – to the Monitoring Body, which may apply the complaints and investigation procedure, as appropriate. Representatives of the Monitoring Body will attend quality assurance meetings and the involvement of the Monitoring Body in the quality assurance process (initial check, attendance at meetings, publication of assured ISPs to the WASPI website) will allow it to identify non-compliance. The Monitoring Body will consult with the appropriate Chair of the regional quality assurance group when determining the appropriate action to address non-compliance.

continued on next page

RQ3 – A COMMITMENT TO THE QUALITY ASSURANCE PROCESS. (PT 2)	
Detail	**RQ3**(ii) Code members must support the quality assurance process in line with the agreed Terms of Reference for their regional quality assurance group. These responsibilities include: • Contributing, participating and attending meetings. Code Members are expected to attend any meeting in which their organisation is taking an information sharing protocol to be assured. • Ensuring that a representative of the lead organisation for each ISP, with sufficient knowledge of the service, project or initiative concerned, be present for the quality assurance of an ISP. [1]
Caveats	Chairs of regional quality assurance groups may agree local arrangements to depart from standardised procedures and attendance requirements. However, this should be in exceptional circumstances.
Monitoring mechanism	-The pre-quality assurance check performed by the Monitoring Body in line with the agreed quality assurance process. - Evidence will be required to be submitted as part of annual assurance and audit processes.
Responsible body	Monitoring Body in the quality assurance process (initial check, and attendance at meetings), and through the annual assurance and audit processes.

[1] A model terms of reference is included Appendix B.

7.4 REVIEWING AND UPDATING AGREEMENTS

The ICO's data sharing code of practice recommends reviewing data sharing arrangements and associated agreements regularly, particularly when a 'change in circumstances or in the rationale for the data sharing arises'. Significant complaints about data sharing or data breaches may also provide a trigger to review agreements. WASPI code members shall review and update agreements in line with the agreed review procedure.

RQ4 – A COMMITMENT TO REVIEW AND UPDATE AGREEMENTS.	
Detail	**RQ4**(i) Code Members shall follow the stipulated review process (see Appendix C). ISPs must be reviewed: • Every two years as a minimum. • Significant changes to the scope of the service varying the volume or type of personal information being shared. i.e an ISP which adds or removes key information sharing stages or significantly changes the partner organisations has taken place. • Where there is a change to the rationale for sharing, which may impact on the lawful basis; for example, a move to / away from consent-based sharing. • When a change to legislation that underpins the sharing (for example, the removal or creation of a legal gateway to sharing) or a change to data protection legislation occurs. • Where a significant (ie reportable) data breach involving the data sharing has occurred or breach of the terms of the ISP. • When the purpose for the information sharing comes to an end. Code Members should make any required updates and ensure all partners have the opportunity to review any changes and provide their input.
Caveats	ISPs which relate to programmes or projects which have a time limited period, i.e 1-3 years, will not be expected to review their ISP in line with the minimum requirements of 2 years, unless a change to processing as stipulated within the requirements applies.

continued on next page

Monitoring mechanism	A register of published ISPs will be made publicly available via the WASPI website. The Monitoring Body produces reports for Quality Assurance Groups, these will include details of any ISPs that have passed their review date or due to expire. Code Members will be expected to demonstrate commitments being taken to review any ISPs due to expire. Monitoring of any ISP six months past expiry will be reported to the WASPI Management Advisory Board. Failure to follow agreed procedures may ultimately result in the application of sanctions.
Responsible body	The Monitoring Body will identify ISPs that have passed the minimum review period and will contact the lead organisation (ISP author and the data protection / information governance lead of the lead organisation) to remind them of the requirement. Failure to commit to undertake a review, or failure to action a review in a timescale set out by the Monitoring Body, may result in the instigation of the complaints and sanction procedure. The Monitoring Body will advise the WASPI Management Advisory Board on any action required to ensure ISPs are reviewed in a timely manner, including the implementation of any sanctions.

7.5 THE PRINCIPLE OF ACCOUNTABILITY

The principle of accountability is a core principle of the UK GDPR. The ICO's data sharing code of practice says that the 'importance of accountability cannot be overstated' and has published an Accountability Framework to provide organisations with guidance on how to demonstrate compliance. The Accountability principles that relate to data sharing form key elements of the code of practice and are reflected in the following requirements.

RQ5 – A COMMITMENT TO SUPPORT AND MAINTAIN DATA SHARING PRACTICES, MAINTAINING DATA SHARING ACCOUNTABILITY CONTROLS	
Detail	**RQ5**(i) Code members shall confirm and, if required, demonstrate that a log of information sharing agreements (including WASPI Information Sharing Protocols) is maintained. **RQ5**(ii) Code members shall be asked to demonstrate appropriate corporate oversight of code compliance and information sharing. To include: • A management framework with escalation and reporting mechanisms. • data protection / Information Governance / Information Management frameworks in place that demonstrate how information sharing procedures are in place across their organisation. • A mechanism for information sharing agreements, to be signed by an appropriate individual within organisations (i.e SIRO, DPO, Caldicott Guardian/Lead, Chief Officer). • Evidence of privacy notices and data protection by design implemented relevant to any data sharing activities subject to the WASPI templates. • Details of how the code member trains all staff who make decisions about data sharing and makes them aware of their responsibilities.

continued on next page

RQ5 – A COMMITMENT TO SUPPORT AND MAINTAIN DATA SHARING PRACTICES, MAINTAINING DATA SHARING ACCOUNTABILITY CONTROLS	
Caveats	None
Monitoring mechanism	The application process will require applicants to demonstrate the governance and accountability measures they have in place to underpin code compliance. All applications will be vetted by the Monitoring Body. An annual declaration of compliance assurance will allow organisations to reconfirm the measures they have in place to underpin code compliance. The annual compliance with code members will be assessed via the Governance & Information Risk Assurance process by the monitoring body. The assessment will require code members to evidence: • How they continue to have controls in place, as set out within their code member application • How they continue to meet the requirements of their code membership, including evidence of activities associated with documented processes set out within ISPs. The annual Governance & Information Risk Assurance will be supplemented with each member being subject to a more exhaustive audit every three years, which will seek to provide additional evidence and assurance of compliance with the code requirements.
Responsible body	The Monitoring Body will review applications and associated evidence. Applications will be considered in line with the application procedure Appendix A.

7.6 CODE COMPLIANCE

Collaboration is an important element of code compliance, members are expected to engage with the monitoring body to allow full application of the procedures and processes associated with this code. All members agree to comply with the monitoring mechanisms established to ensure compliance with the code. Failure to follow agreed processes and procedures may result in the application of sanctions. Failure to comply with sanctions may result in escalation to the Information Commissioner's Office.

RQ6 – COMPLY WITH IDENTIFIED MONITORING MECHANISMS, COMPLAINT PROCEDURES AND OTHER ELEMENTS OF THIS CODE, INCLUDING ANY APPLIED SANCTIONS	
Detail	**RQ6**(i)On request, all code members will provide information to the Monitoring Body to allow: • Applications for code membership to be accurately assessed. • The effective monitoring of the requirements of this code. • The effective implementation of the complaints and sanction procedure and any other procedures associated with this code.
Caveats	No request for information shall interfere with or compromise any ongoing investigation or audit by a regulatory or statutory body, or any current or potential legal proceedings.
Monitoring mechanism	Failure to engage with the process and procedures associated with the code will be recorded by the monitoring body and reported to the WASPI Management Advisory Board. Failure to complete and provide evidence of assurance as part of the annual Governance & Information Risk Assurance The complaints and sanctions procedure may be implemented.
Responsible body	The Monitoring Body will note instances of non-compliance and apply the complaints and sanctions procedure, as appropriate.

Section 8 - Monitoring and the monitoring body

8.1 OVERVIEW OF THE MONITORING APPROACH

Article 40(4) of the UK GDPR states that codes of conduct shall contain mechanisms that enable a monitoring body to carry out mandatory monitoring of compliance with a code's provisions. This monitoring does not prejudice the tasks and powers of the Information Commissioner's Office.

Article 41 sets out the requirements for a monitoring body. However, Article 41(6) creates a point of difference in relation to the monitoring requirements for code members that are public authorities / public bodies[2], and other code members. That is, while a monitoring body is required to monitor code compliance by non-public bodies, it is not required to monitor compliance by public authorities / public bodies. The rationale for the different monitoring requirements is that public authorities / public bodies are subject to internal and external compliance audits, as well as statutory governance requirements that should ensure compliance with any relevant standards or codes.

For the sake of clarity and to ensure monitoring arrangements are effective and fair, for the purposes of this code:

- **There shall be a monitoring body, which will monitor compliance with this code by all code members.**
- **All code members will be subject to monitoring regardless of whether their organisation is a public authority / public body.**

Monitoring mechanisms will be consistent for all code members and will not interfere with any other regulatory or statutory auditing that any public bodies may be pertinent to. Monitoring information may be shared with any such bodies where applicable, information may also be shared from regulators or other agencies with the monitoring body where such bodies may have concerns over a code members obligations with this Code of Conduct.

[2] See the definition provided by the Freedom of Information Act 2000.

This code builds upon and expands existing mechanisms used to maintain the integrity of WASPI. Although a code cannot be approved without identifying monitoring and enforcement mechanisms, wherever possible compliance with the requirements of the code will be promoted through the collaborative approach developed with WASPI stakeholders over many years.

Formal measures, such as sanctions or exclusion from the code, will be taken as a last resort and where agreement regarding changes to behaviour and practices cannot otherwise be agreed. Formal measures will be proportionate to the nature of any breach and will be aimed at ensuring code compliance rather than punitive in nature. Specific monitoring mechanisms and further details about the monitoring body are included below.

Monitoring processes, including those of declaration of compliance assurance are designed to provide support to organisations and provide assurances to the monitoring body that code members are maintaining standards.

To support this an annual assessment will be required to be completed by each code member. This assessment known as the **Governance & Information Risk Assurance (GIRA)** will allow for continued evidence to be provided and assessed to demonstrate that code members are maintaining standards of assurance expected of them.

This process will not only seek assurance that templates, processes and governance for data sharing are being adopted but will provide mechanisms for monitoring that the practices of code members, described within information sharing protocols, remain accurate and up to date. For example, code members will be expected through this process to provide evidence of how they are applying WASPI, submitting evidence of data protection by design and by default and transparency linked directly into ISPs as well as demonstrating how they are embedding the application of the code within their organisation.

8.2 GOVERNANCE & INFORMATION RISK ASSURANCE (GIRA)

The GIRA will be a required annual assessment which will be reviewed by the monitoring body in respect of each code member.

The GIRA will focus on monitoring and measuring that a code member continues to meet standards expected and to provide evidence of its organisational controls aligned to the WASPI code of conduct and to ensure that documented processes set out within ISPs are consistent with organisations record of processing activities.

It will also focus on the code member submitting evidence which demonstrates how they are meeting the code requirements and providing details that demonstrate that they are following the data sharing activities outlined within ISPs, for example requiring evidence of privacy notices or equivalent relevant to existing assured ISPs, together with setting out evidence of the data flows and systems used which are documented within ISPs.

The GIRA will be completed in advance of annual membership expiring, a minimum of 8 weeks prior to expiration of membership but no sooner than 12 weeks before expiration, as a self assessment return and this will be considered by the monitoring body to determine if appropriate evidence has been provided that demonstrates that the code member remains compliant with the code of conduct requirements. The monitoring body will maintain a record of the assessment and evidence provided and this may be considered as part of future assessments or to consider any complaints made against the code member. This information may also be shared with any other regulatory bodies as part of audits and inspections obligations they may have, for example Audit Wales and Care Inspectorate Wales.

To supplement the assessment of the GIRA, the monitoring body will undertake a comprehensive audit programme with the commitment that each code member would be subjected to a more exhaustive audit at a minimum of every three years. This audit will consist of supplementary evidence, from evidential meetings and inspections between the monitoring body and code member to enable assurance of controls and standards in place which supplement the code members GIRA.

8.3 THE MONITORING BODY

For the purposes of this code, the WASPI Team, is the monitoring body. Article 41(2)(a) of the UK GDPR states that the monitoring body should demonstrate its independence, which can be demonstrated within four main areas:

i) legal and decision-making procedures,

ii) financial,

iii) organisational and

iv) accountability.

The WASPI Team, sits within the line management structure of the Information Governance team of Digital Health and Care Wales (DHCW), a statutory body[3]. The decision-making process and escalation points for WASPI are clear and separate to the line management structure of DHCW. As such, the WASPI governance structure allows the monitoring body to function independently.

In addition, DHCW is not a public facing organisation and does not generally provide services directly to citizens. The monitoring body has a line of escalation into Welsh Government policy leads through to the Minister for Health and Social Services. WASPI has its own website, separate from others operated by DHCW, which is used to host documentation, a library of good practice and details of code members.

[3] Established under 'The Digital Health and Care Wales (Establishment and Membership) Order 2020'.

Actual or perceived conflicts of interest between the WASPI Team, code members and other stakeholders (including DHCW) can be minimised and mitigated through measures that include:

- Transparency; reporting the outcome of investigations or monitoring reports to the DHCW Executive Management Board will allow scrutiny of the actions of the WASPI Team.
- Encouraging dialogue between code members to resolve issues informally will reduce the likelihood of more formal complaints and the need for formal investigations that might lead to conflicts of interest. This a continuation of the approach taken to develop and establish WASPI.

Any information gathered as part of monitoring activities will be held by the monitoring body, on DHCW digital infrastructure, for at least the duration of the relevant organisation's code membership. Such information will only be shared with other parties, such as the WASPI Management Advisory Board, the relevant Regional Quality Assurance Group and the ICO, to the extent that such sharing is required to effectively investigate alleged code breaches, to implement sanctions or to otherwise comply with the requirements of a code of conduct. The monitoring body will report any substantial changes (such as change in its legal, commercial, ownership or organisational status and key personnel, resources, locations and any changes to the basis of accreditation) to the ICO immediately and without undue delay. Substantial changes will result in a review of the ICO's decision regarding accreditation.

The WASPI Team are trained to nationally recognised qualifications in data protection and DHCW are committed to ensuring that the team continue to maintain professional qualifications.

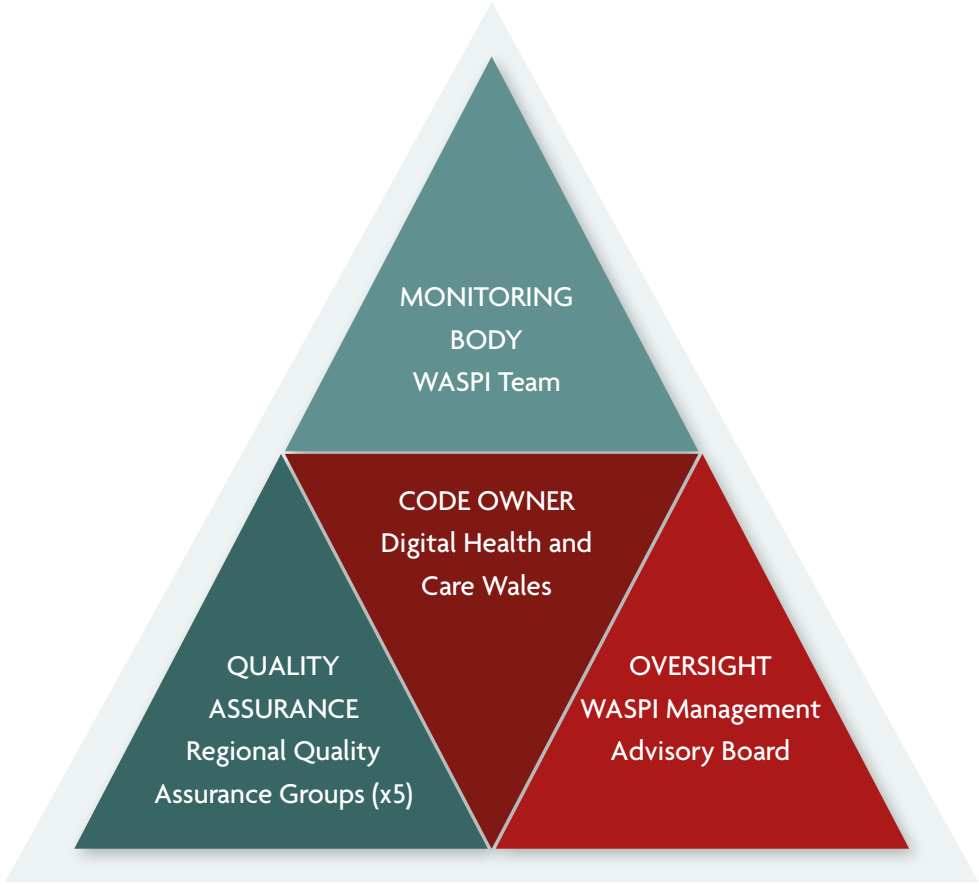
8.4 DELIVERY OF MONITORING BODY FUNCTIONS

Digital Health & Care Wales and Welsh Government will provide the WASPI Team with sufficient capacity and tools to fulfil its monitoring body and code owner obligations. These resources and tools will be provided to the WASPI Team who will ensure that procedures are in place for managing and maintaining all aspects of their responsibilities, including by not limited to:

- The code member application processes. This will be achieved through online and offline applications which will be assessed by the WASPI Team.
- Annual assurance of code members. This will be measured through annual GIRA assessments which will be issued to each code member and assessed and determined by the WASPI Team, with the team also providing an audit function.
- Reporting and monitoring against ISP developments and regional quality assurance groups. This will be achieved from monitoring systems and tools to enable reporting to the WASPI Management Advisory Board for an oversight of code member compliance.
- Handling of appeals, complaints and sanction processes. A webpage on the WASPI website will be provided with transparent information for organisations and the public and procedures will be adopted and published in respect of each process.
- The WASPI Team will manage all communications to the ICO, including that of any infringements that lead to suspensions or exclusions of code members as well as providing annual reporting.
- The WASPI Team shall provide the code owner and ICO with an annual report on the operation of the code as set out in appendix E of this code.
- The WASPI Team will consider the need for this code to be reviewed via completion of the annual report to the ICO, as set out in appendix E of this code.

Section 9 – Governance, roles and responsibilities

The diagram below sets out the WASPI governance structure, followed by a table that explains roles and responsibilities.



WASPI Governance

CODE GOVERNANCE

WASPI Management Advisory Board	Is provided with information as oversight that the code owner, monitoring body and code members meet their obligations
Digital Health and Care Wales (Code Owner)	Acts as the code owner and ensures the code is periodically reviewed and that capacity and tools are provided to the Monitoring Body to discharge their responsibilities. Ensures any amendments or extensions to the code, and changes or additions to the monitoring body, are approved by the ICO. As Code Owner provide an annual report to the ICO to include a list of current code members and any new members, information concerning code member breaches of code requirements, details of any members suspended and outcomes of the code review.
Regional Quality Assurance Groups	Quality assure ISPs. Implement regional standards as expected through their terms of reference. Discuss potential instances of non-compliance with the code and escalate as required. Discuss and agree, as appropriate, priorities for the review and update of agreements.
WASPI Team/ Monitoring Body	Acts as the monitoring body including responsibility for the Governance & Information Risk Assurance and audit processes. Considers and approves applications for code membership, providing oversight of code compliance to the WASPI Management Advisory Board. Supports regional quality assurance groups and the WASPI Management Advisory Board Monitors compliance with code members obligations as required within the code monitoring mechanisms and investigates complaints of non-compliance Reviews and verifies the outcome of complaints, monitoring activity and any sanctions. Directs reviews and approves changes to the code in consultation with the ICO.

Section 10 – Scope

10.1 TERRITORIAL SCOPE

This code is a national code applicable within the United Kingdom. It is targeted at service providers in Wales but complies with UK data protection legislation and the Information Commissioner's Data Sharing Code of Practice. As such, the Information Commissioner's Office (ICO) is the relevant supervisory authority.

10.2 PROCESSING SCOPE

This code supports the sharing of personal data, between members and other stakeholders, for the purposes of providing services that, either directly or indirectly, deliver, support or promote the health, wellbeing, education, security and safeguarding of citizens in Wales. This code applies to controllers as defined by data protection legislation, either acting alone or jointly.

Nothing in this code shall constitute, create or otherwise give effect to a joint venture, pooling arrangement or partnership or similar arrangement between code members, the code owner, any monitoring body nor any other party. Nothing in this code is intended as, or shall be construed to create, a relationship of agency between the parties. Accordingly, members shall not have any authority to act or make representations on behalf of another member, and nothing herein shall impose any liability on any party in respect of any liability incurred by any other party to any third party.

10.3 APPLICABILITY OF THE CODE

The concept of approved codes of conduct is provided by article 40 of the UK GDPR. There is no equivalent provision in part 3 of the Data Protection Act 2018 (DPA 2018). The principles of UK GDPR and the DPA 2018 are closely aligned and compliance with this code will therefore help demonstrate compliance with both pieces of legislation. Most organisations processing personal data for the law enforcement purposes also process data for non-law enforcement purposes and information sharing agreements developed using WASPI often include a combination of lawful bases from UK GDPR and DPA 2018. As such, code membership provides benefits to **all organisations** delivering the types of services to the people of Wales.

10.4 GOVERNANCE OF THE CODE IN EXCEPTIONAL CIRCUMSTANCES

In the unlikely event of accreditation of the code being revoked, DHCW's WASPI Team will continue to manage and monitor all governance to the same level and expectations as set out as if this code was still applicable.

In the unlikely event of the monitoring body being revoked, DHCW as the code owner, will work to ensure that a replacement monitoring body will be identified as soon as possible with a view to an application for accreditation being made to the ICO within six months unless otherwise communicated.

Section 11 – Complaints and Code Member Sanctions

Developing WASPI into an approved code of conduct provides the opportunity to reinforce the positive behaviours that helped to embed WASPI across Wales. While it is anticipated that stakeholders will continue to resolve most issues through discussion, a code requires clear mechanisms to deal with infringements. Sanctions are also a requirement of a code.

11.1 COMPLAINT ABOUT/INFRINGEMENTS BY CODE MEMBERS

The WASPI Team within DHCW (as the monitoring body) will undertake investigations into alleged or possible infringements of the code. Alleged infringements can be brought to the attention of the monitoring body via complaints, which can be submitted to waspiservice@wales.nhs.uk. The monitoring body may otherwise become aware of possible infringements – for example, via feedback from quality assurance groups or from the ICO – and may decide to investigate at its own discretion.

The investigation process will commence with the nature of the alleged / possible infringement being provided in writing to the relevant code member(s). Code members must comply with any reasonable request for information to assist with the investigation. Investigations may be conducted through a review of paper/electronic information and may be supplemented through discussions and meetings (notes of which shall be produced), as agreed between the code member and the WASPI Team. The outcome of investigations will be:

1. **No infringement identified.** The code member will be notified of the outcome in writing.
2. **Infringement identified, informal outcome.** The code member agrees to take corrective action. The code member will be notified in writing of the infringement and agreed corrective action.

3. **Infringement identified, formal outcome.** The code member disagrees with suggested corrective action. The code member will be notified in writing of the infringement, any required corrective action and the timescale within which corrective action must be taken. The code member will confirm in writing that it has taken corrective action.

4. **Infringement identified, formal resolution, sanction applied.** Likely to apply where there has been a serious infringement of the code or the code member has failed to comply with previously identified corrective action. The code member will be notified in writing of the sanction, including any timescale and any corrective action that can result in the sanction being lifted. The code member will confirm in writing that it has taken corrective action.

11.2 SANCTIONS

The application of sanctions will be made by the monitoring body only with the WASPI Management Advisory Board being provided with details of any sanctions applied. Any member of the Management Advisory Board directly affected, or otherwise declaring an interest, shall not be involved in discussions regarding complaints, investigations and sanctions.

The details of any sanction will be provided in writing to the relevant code member (to the contacts provided on the application form) by the monitoring body. The written notice will include:

- The nature of the infringement.
- The decision of the monitoring body and any evidence that supports its decision.
- The nature of the sanction and its conditions; for example, whether it will be lifted after a period of time or after remedial action on the part of the code member.
- Any right of appeal.

Sanctions will include:

- Informal discussion or advice.
- Improvement action issued in writing requiring improvement measures to be put in place, i.e training staff on WASPI requirements, agreeing a date for improvements with updating ISPs to take place.
- Suspension as a Code Member.
- Application for membership rejected.

Examples of sanctions & corrective actions are provided in appendix D of this code.

11.3 REPORTING

The monitoring body will provide the DHCW Executive Management Board and WASPI Management Advisory Board with regular overview of reports on complaints, investigations and outcomes, including any trends. The ICO will be informed of any sanctions applied to code members which have resulted in suspension, exclusion or the lifting of any sanctions against code members. Further detail on review of the code and reporting are provided at appendix E of this code.

11.4 APPEALS

Appeals against the outcome of an investigation can be made in writing to the monitoring body, via the following email address waspiservice@wales.nhs.uk. The decision of the monitoring body will be provided in writing and will be final.

11.5 COMPLAINT ABOUT THE MONITORING BODY

Any complaints about the monitoring body can be made in writing to the code owner via the following email address dhcwinformationgovernance@wales.nhs.uk marked for the attention of the WASPI code of conduct code owner.

11.6 COMPLAINT ABOUT THE CODE OWNER

Any complaints about the code owner can be submitted to the monitoring body via the following email address waspiservice@wales.nhs.uk, which will liaise with the ICO to determine the appropriate course of action.

Appendix A – Applications and ending code membership

Applicants for code membership must read and understand the code and its requirements prior to completing the application form. **Completion of the pre-application checklist is recommended.** Adherence to this code should not result in any organisation facing a conflict with any internal policies, procedures or standards. Any such conflict should be resolved before applying for code membership.

Any information you provide as part of the application process will be used for the purposes of assessing your organisation's application for code membership and maintaining a register and lists of code members and contact information. If your application is successful, the monitoring body will include your organisation in a public list of code members and provide a WASPI code of conduct badge which organisations will be permitted to display. The monitoring body will report membership to the Information Commissioner's Office.

The application process does not represent an audit of prospective members' data protection practices, nor does acceptance for code membership provide a quality seal, certification or other quality standard. The application process considers the suitability of an organisation for code membership. If accepted for code membership, adherence to the provisions of the code will help members comply with data protection legislation, taking into consideration the scope of the code.

APPROVED APPLICATIONS

Approved applications will be confirmed by email using the contact details provided on the application form. New members (organisation name) will be added to the list of code members on the WASPI website and be provided a badge to use as evidence of their compliance. Additionally, members will be added to a mailing list for the WASPI newsletter. At any time, an individual can opt out of receiving communications by emailing: waspiservice@wales.nhs.uk.

REFUSED APPLICATIONS

The WASPI Team will endeavour to engage with organisations prior to refusing an application. This could result in the application being approved (for example, following clarification of queries), a withdrawn application (with the option to resubmit when the organisation is able to evidence its suitability for membership) or a refused application. Refused applications will be confirmed by email using the contact details provided on the application form. Reasons for a refusal will be provided. Refusal of an application for membership does not preclude the resubmission of a subsequent application.

APPEALS

An appeal against a decision to refuse code membership can be submitted by email to waspiservice@wales.nhs.uk. An appeal should include the name of the organisation, the reason for the appeal and any relevant supporting evidence. Appeals will be escalated within the WASPI Team structure for a final decision. There shall be no further right of appeal.

ENDING MEMBERSHIP

A Chief Officer / Chief Executive or equivalent may end their organisation's membership of this code at any time by writing to the WASPI Team. To withdraw membership, an email must be sent to waspiservice@wales.nhs.uk. The date of withdrawal will occur when it is actioned by the monitoring body and a response by email will be provided confirming the ending of membership with any remaining steps (such as cease of using the badge as evidence of compliance with the code). Organisations ending their code membership will not prejudice their signatory to the Accord unless otherwise stated by the organisation. Withdrawals from code membership will be reported to the ICO as part of regular reporting requirements.

CONTACT

Any queries about this procedure should be emailed to the WASPI Team: waspiservice@wales.nhs.uk.

PRE APPLICATION CHECKLIST

Please complete this checklist prior to completing and submitting your application for code membership.

The pre application checklist is for your own purposes and it does not need to be submitted as part of the application if you decide to proceed.

Completing the pre application checklist will help potential applicants determine whether their organisation is ready for, and will benefit from, code membership. You should be able to answer yes to the following questions to achieve code membership.

Does your organisation regularly design and/or deliver collaborative services to citizens in Wales? *If not, code membership may not offer significant benefits over and above those offered by standard WASPI membership.* *Please refer to the code for details of the potential benefits of code membership.*	Yes/No
If required to do so, has your organisation registered with the ICO? *You will be asked for your registration number (if relevant) as part of the application process.*	Yes/No
Is your organisation a signatory to the WASPI Accord? *If you have answered no, please complete the WASPI Declaration of Acceptance and Participation (available on the WASPI website) before submitting your application for code membership. This will confirm you as a WASPI Member prior to your application to become a WASPI Code Member.*	Yes/No
If required to do so, has your organisation designated a Data Protection Officer (DPO)? If not (and not required to designate a DPO) has your organisation identified an individual who has overall responsibility for the personal data it processes? *Before applying for code membership, you should identify a senior person with responsibility for the personal data processed by your organisation.*	Yes/No

Has your DPO (or equivalent, if not required) and your senior management team/board/executive approved the decision to apply for code membership? *Senior level engagement is an important element of data protection compliance and accountability. You should ensure senior management is aware of the proposed application. Your lead officer, with responsibility to sign on behalf of the organisation, will be required to sign the application form.*	Yes/No
Can your organisation demonstrate key elements of accountability in relation to information sharing? For example: • A log of information sharing agreements. • A governance structure with escalation and reporting mechanisms. • A policy or policies that adopt and promote "data protection by design and default" as set out in Article 25 of UK GDPR. • A mechanism for information sharing agreements to be signed by an appropriate individual. • Guidance and/or training for staff involved in information sharing on data protection / information governance responsibilities. *Accountability is a key principle of data protection compliance. The application process will require you to demonstrate how your organisation can demonstrate accountability in relation to its information sharing practices. Please refer to the full application form for further details and contact the WASPI Team with any further questions waspiservice@wales.nhs.uk*	Yes/No

APPLICATION FORM

Application form for WASPI code membership

Appendix B – The quality assurance process & model terms of reference

The folowing documents will be available on the WASPI website:

Procedure for the quality assurance of Information Sharing Protocols

Wales Accord in the Sharing of Personal Information Terms of Reference for Quality Assurance

Appendix C – A process for reviewing ISPs

Out of date Information Sharing Protocols and other agreements present a compliance risk and can undermine public confidence that their personal data is being appropriately and lawfully processed. Code members are required to regularly review and update their agreements, including quality assured ISPs. The process for reviewing and updating ISPs is as follows:

Start:

1. ISP Quality assured. The author sets the review date, which must be included in the final version. ISPs must be reviewed two years from the date the agreement is assured but the context of the service should be considered. For example, an ISP that supports a dynamic service with process and partners that are subject to change may need to be reviewed.

2. ISP authors should ensure review dates for ISPs and other agreements are recorded and reviewed by their respective organisations and that there is a mechanism to trigger a review. The monitoring body has formal mechanisms for review of ISPs which are due to expire, or past expiry and the lead author organisation will be expected to demonstrate measures in place to ensure that the review process is initiated.

3. Events that trigger a review of an ISP:

    - The passage of time. As a minimum standard, ISPs should be reviewed two years after the approval date (the date approved by the relevant Quality Assurance Group) or sooner if one of the following triggers applies.

    - A significant change to the service, which adds or removes key information sharing stages or significantly changes the partner organisations.

    - A change to the rationale for sharing, which may impact on the lawful basis; for example, a move to / away from consent-based sharing.

- A change to legislation that underpins the sharing (for example, the removal or creation of a legal gateway to sharing) or a change to data protection legislation.
- The end of a service. This may result in the agreement being terminated and the creation of a new agreement to reflect any amended process.

4. ISPs authors are responsible for ensuring regular reviews of ISPs. A review should consider the following questions:

- Has the purpose of processing changed?
- Do the information sharing partners need to be updated?
- Is the lawful basis for processing still relevant?
- Have the key information exchanges or the categories of information changed (in which case you will need to update the information reference table)?
- Have there been any changes to legislation which underpins to information sharing exchanges?
- Is a newer version of the WASPI template available, in which case, it should be used when the ISP is reviewed.

5. The author should make any required updates and ensure all partners have the opportunity to review any changes and provide their input.

6. All amended ISPs will be subject to a level of quality assurance. The ISP author should refer to the ISP quality assurance procedure. The Chair of the relevant quality assurance group and the WASPI Team will determine the extent to which a reviewed ISP needs to be quality assured dependant on the changes made.

7. Monitoring of adherence to the requirement to review and update ISPs, and any other form of agreement which may be subject to quality assurance, will be monitored by the WASPI Team.

- Regular reports of ISPs with a last assured date >two years will be provided to members of quality assurance groups for consideration, and this will be reported by the monitoring body to the WASPI Management Advisory Board.
- For ISPs with a last assured date of >two years and two months, specific, reminders will be sent to i) ISP authors ii) Information Governance/Data Protection leads iii) Data Protection Officers with a reminder of the need to ensure the agreements are reviewed, or the WASPI Team is informed they are no longer extant.
- Formal investigations – which may ultimately result in sanctions – may commence for any members who authored an ISP with a last assured date of >two years and 6 months. Investigations of code members whose organisation maybe part of an ISP, not the lead author, but whose actions may be causing failures for the author code member, may also be applicable.

Appendix D – Examples of Sanctions & Corrective Actions

The table below includes examples of behaviour that does or does not constitute a breach of the code or an infringement and the possible corrective action or sanctions that could apply. This is non exhaustive list. Code members should be clear on the requirements of the code, including to comply with any investigation process, prior to applying for code membership.

Activity	Code infringement?	Corrective action	Possible sanction	Who is responsible?	Comments
Failure to meet the application pre-requisites	No	Demonstrate the applicant can meet the pre-requisites and resubmit application.	Application for membership rejected.	Monitoring Body.	Decision can be appealed or application resubmitted.
Disagreement regarding the content of an Information Sharing Protocol	No	To be resolved through discussion between code members, the WASPI Team (if required) and quality assurance groups (if required).	None	Partners to the agreement. Monitoring Body (if required). Quality Assurance Group (final approval of ISPs).	If relevant, requests for changes to standard templates can be submitted to the WASPI Team who will consider with support from the WASPI Management Advisory Board.

Code member does not use WASPI templates (where available and relevant to the sharing in question) to underpin information sharing arrangements.	Yes	The code member agrees to implement the appropriate WASPI template, with support if required.	First instance / complaint: Informal discussion or advice. Second instance / complaint: WASPI Team discusses the issue with the code member and sets out the possibly infringement in writing. Persistent breach: Infringement investigation process. Possible suspension for a set period or until a change in behaviour is evidenced, or expulsion for repeated behaviour	Monitoring Body WASPI Team. WASPI Team	It is anticipated that sanctions of suspension of code membership or expulsion will be infrequently used.
Code member does not adhere to the agreed quality assurance process.	Yes	The code member adheres to the quality assurance process with support from the Monitoring Body and members of the relevant quality assurance group (for example a discussion about the process and procedure), as appropriate and agreed.	As Above	As Above	As Above

Code member does not actively review and update ISPs and other agreements (as evidenced by the online register).	Yes	The code member implements processes and procedures that facilitate the review of agreements within agreed timescales.	As above.	As above.	As above.
Code member does not assist the Monitoring Body in any investigation.	Yes	The code member provides the requested information.	As above.	As above.	As above.

Appendix E – Review of the Code and Annual Reporting

REVIEWING THE CODE

Any approved code of conduct must be periodically reviewed to ensure it remains relevant and up to date.

A review of the code will be considered as part of the annual reporting to the Information Commissioner's Office. If the code owner feels there may be a requirement to review the code this will be referred to the monitoring body.

Any significant changes to data protection legislation, or changes to the application or interpretation of the law that, that may impact on the code will require the code to undertake a review.

A review of the code may be required if any requirements or instructions are issued to the code owner by the Information Commissioner.

A review of the code may be required if the WASPI framework, monitoring body or code owner changes to the extent that the code requires a review.

ANNUAL REPORTS

The monitoring body will provide the code owner and the WASPI Management Advisory Board, Quality Assurance Groups and code members with an annual report (to be published to the WASPI website) on the operation of the code. The report shall include:

- information concerning new members to the code.
- details of any suspensions and exclusions of code members;
- confirmation that a review of the code has taken place in line with the agreed triggers.
- that there are no substantial changes to the monitoring body.
- information concerning data breaches by code members, complaints managed and the type and outcome of monitoring functions that have taken place.

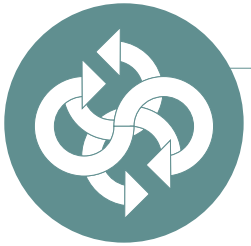
Appendix F – WASPI templates & consultation plan

The folowing documents will be available on the WASPI website:

Information Sharing Protocol Template

Consultation & Communication Strategy

Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information



AELOD COD YMDDYGIAD
CODE OF CONDUCT MEMBER

Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information

Document version 1.0