

Meeting of:	<b>Cabinet</b>
Date of Meeting:	<b>Monday, 18 March 2019</b>
Relevant Scrutiny Committee:	Corporate Performance and Resources
Report Title:	Update on the Wales Accord on Sharing of Personal Information (WASPI)
Purpose of Report:	To advise Members of an update to the Wales Accord on Sharing of Personal Information (WASPI) and to obtain authority to sign the new version of the Accord and implement its requirements.
Report Owner:	Executive Leader and Cabinet Member for Performance and Resources
Responsible Officer:	Carys Lord, Head of Finance/Section 151 Officer
Elected Member and Officer Consultation:	Monitoring Officer/Head of Legal and Democratic Services Operational Manager (Democratic Services)
Policy Framework:	To comply with statutory obligations upon the authority. This is a matter for Executive decision by Cabinet, save for amendments to the Council's constitution.
<p>Executive Summary:</p> <ul style="list-style-type: none"> <li>The Council has previously signed the Wales Accord on Sharing of Personal Information. This ensures that any sharing is appropriate and individuals' legal rights are respected. It set out a procedure and mechanism and is endorsed by the Information Commissioner's Office. The scheme has recently been updated and this report seeks authority for the Council to sign the new version of the accord. It sets out the process and procedures for practical implication of the requirements, including relevant delegations to chief officers.</li> </ul>	

## **Recommendations**

1. That the contents of this report are noted.
2. That the organisational requirements as set out within the Accord be implemented.
3. That the Managing Director be given delegated authority to sign the latest version of The Wales Accord on Sharing of Personal Information (WASPI) on behalf of the Council as required in paragraph 1.3.1 of the Accord.
4. That the Information Manager (Lawyer) be the Designated Person as required under paragraph 1.3.3. of the Accord in order to ensure compliance with its commitments.
5. That Chief Officers be given delegated authority to enter into Data Sharing Agreements not within the WASPI template provided such agreements have been approved by the Monitoring Officer/Head of Legal and Democratic Services in consultation with the Head of Finance/Section 151 Officer and the Data Protection Officer. Paragraph 2 of the Delegation to Chief Officers in the Council's Constitution be amended in this respect.
6. That Chief Officers be given delegated authority to enter in Data Disclosure Agreements and Joint Data Controller Agreements provided such agreements have been approved by the Monitoring Officer/Head of Legal and Democratic Services. Paragraph 2 of the Delegation to Chief Officers in the Council's Constitution be amended accordingly.
7. That the report be referred to Council, in pursuance of recommendations 5 and 6 in relation to amendments to the Council's Constitution.

## **Reasons for Recommendations**

1. To advise Members of the Update.
2. To practically implement the requirements of the Accord.
3. To ensure WASPI is practically implemented. The consultations as set out in the recommendations are appropriate as the Head of Finance/Section 151 Officer is the Council's Senior Information Risk Owner and Data Protection Officer is required under the General Data Protection Regulation (GDPR) to be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
4. To ensure that the Council's Constitution can be properly amended.

## **1. Background**

- 1.1 Sharing of personal information to deliver effective and efficient public services is an essential element of Welsh Government Policy. Equally, the Council's Corporate Plan places emphasis on partnership working with key public sector organisations. Data Protection Legislation requires personal information which is shared is done fairly and lawfully. The General Data Protection Regulation implemented in May 2018 together with the new Data Protection Act updated the Data Protection Laws.

- 1.2 In Wales the scheme known as the Wales Accord on Sharing of Personal Information (WASPI) was initially introduced by Welsh Government. It sought to practically implement this and the Accord was established to ensure that data sharing was done lawfully and fairly and in accordance with the Data Protection Legislation.
- 1.3 Whilst the scheme is voluntary a large number of public sector organisations have signed up to it, notably most Local Authorities in Wales, Health Boards and others such as doctors' surgeries.
- 1.4 The scheme works on two levels, firstly participating organisations signing an Accord to confirm their commitment to sharing information under the Scheme. Secondly, an Information Sharing Protocol template. This is a form which incorporates the Data Protection requirements for data sharing and sets out the practicalities of data sharing such as "what, when, how and who" information will be shared with. This would be completed by individual services. Data Disclosure Agreements are for one way sharing and Joint Data Controller Agreements have recently been added to cover these forms of sharing.

## **2. Key Issues for Consideration**

- 2.1 This Council originally signed up to the WASPI Accord in 2011.
- 2.2 Since then, the Authority has entered into a number of data sharing arrangements in accordance with the WASPI requirements. Many of these have been in Social Services context.
- 2.3 The introduction of the GDPR and feedback in relation to the previous scheme necessitated a revision of the WASPI forms. Accordingly, WASPI have issued a new Accord and a new set of templates.
- 2.4 Attached at Appendix 1 is the new Accord for WASPI. The Accord sets out in Section 2, a number of organisational commitments which the Council has to adhere to comply with the requirements. In particular of note are the following:
  - Data Subject Rights - there is commitment that each organisation will allow data subjects to exercise their rights fairly and consistently. Specific mention of the right to be informed is made in that organisations must be clear, open and transparent with data subjects about the collection and use of their personal information;
  - In relation to the legal basis for sharing personal information, the Accord requires each organisation shall ensure an appropriate legal basis has been established and documented;
  - In relation to staff and others with access to information, the requirement is that organisations must have in place their own operational policies and procedures to facilitate the effective processing of personal information and to support its staff to share information appropriately, safely and lawfully;
  - Staff contracts must contain appropriate confidentiality clauses;
  - Each organisation must have in place disciplinary procedures to be invoked if a member of staff is found to have breached confidentiality of an individual;

- Each organisation must ensure staff with access to personal information receive an appropriate level of training, advice and support;
  - Appropriate contractual data processing confidentiality agreements must be in place to underpin the processing of personal information by third parties/processors;
  - In respect of records management, of note is that each organisation will take reasonable steps to advise any other party known to have received or be holding inaccurate personal information;
  - All participating organisations will have in place policies and procedures, in relation to retention, storage and disposal of records;
  - Under the Information Security and Risk Management section each organisation must have in place a level of security commensurate with the sensitivity and classification of the information it processes;
  - Before developing and implementing new systems/working practices that process personal information each organisation must consider the impact on individuals' privacy. Data Protection Impact Assessments (DPIAs) should be undertaken where necessary;
  - Any concerns or complaints received from individuals about the processing of their personal data will be dealt with promptly and in accordance with the internal complaints procedure of the partner organisations;
  - All partner organisations must put in place processes that allow concerns about non-compliance with this framework to be reported to the Designated Person.
- 2.5** Authority is now sought for the Managing Director to sign the Accord on behalf of the Council in order for the Authority to continue to take part in the Scheme.
- 2.6** Many of the organisational requirements are consistent with the work the Council has done in relation to implementing the GDPR and the Data Protection Act however, further work will be needed to cross reference this and in particular staff awareness/training of the new Accord will need to take place. The Council's StaffNet will need to be updated. It is essential that Officers recognise when data sharing can take place and know the mechanisms to implement it.
- 2.7** Chief Officers currently have delegated authority to enter into data sharing agreements where necessary and appropriate in the form of the WASPI template, however, WASPI primarily applies to Wales and in some instances data sharing takes place with organisations outside Wales. Accordingly authority is sought for Chief Officers to enter into those agreements where necessary and appropriate. Data Disclosure Agreements and Joint Data Controller Agreements have been added to the WASPI documentation since the last version and accordingly it is appropriate that they are included.

### **3. How do proposals evidence the Five Ways of Working and contribute to our Well-being Objectives?**

**3.1** In the longer term, the adoption of the WASPI Accord will ensure individuals rights are protected on the sharing of information and will prevent the inappropriate sharing of information.

#### **3.2**

Through the issue of privacy notices, individuals will be involved in how their personal data is used by the Authority.

### **4. Resources and Legal Considerations**

#### **Financial**

**4.1** To date, all WASPI implementation has taken place within budget, however with the further work needed this will be subject to further review.

#### **Employment**

**4.2** To date, all WASPI implementation has taken place within budget, however with the further work needed this will be subject to further review.

#### **Legal (Including Equalities)**

**4.3** It is a requirement to share data fairly and lawfully and in accordance with the law.

### **5. Background Papers**

The Wales Accord on the Sharing of Personal Information Version 5

The Vale of Glamorgan Corporate Plan 2016-20

The General Data Protection Regulation 2016

The Data Protection Act 2018



## Wales Accord on the Sharing of Personal Information

# The Accord

For organisations involved in the protection, safety, health, education and social welfare of people in Wales

(including statutory, private and third sector organisations)

# Contents

<b>Forewords</b>	<b>2</b>
<b>1 Introduction and Purpose</b>	<b>4</b>
1.1 Introduction	4
1.2 Framework Documentation	5
1.3 Adoption of the Accord	5
<b>2 Organisation Commitments</b>	<b>6</b>
2.1 Introduction	6
2.2 Data Subjects' Rights	6
2.3 Legal Basis for Sharing	6
2.4 Staff and Others with Access to Information	6
2.5 Records Management	7
2.6 Information Security and Risk Management	7
2.7 Complaints and Concerns	8
<b>Annex 1 – Glossary of Terms</b>	<b>9</b>

# Forewords

Sharing personal information to deliver effective and efficient public services is an essential element of Welsh Government policy. We are also acutely aware that third sector and commercial organisations also need to share personal information to enable effective service delivery.

Empowering staff to share appropriate information with the right person at the right time, is a key principle to delivering effective services; we must ensure that these staff can focus on providing care and support with the confidence that they can do so correctly, legally and with the support of their employers. Similarly, the public must have the confidence that the staff are sharing appropriately and organisations need to have assurance that relevant legal considerations are addressed, and risks identified and mitigated.

The further development of the Wales Accord on the Sharing of Personal Information (WASPI) has been driven by the changing legislative environment and feedback from those who use the framework. It continues to provide an established, recognised and robust good practice approach to information sharing which staff, citizens and all service partners can have confidence.

The Information Commissioner's Office has been integral to the review and update of the WASPI framework, working alongside the various partners to provide an improved and versatile framework that meets the needs of the new legislation and those who use it. I would urge all organisations involved in the delivery of services to people to commit to its use, to make the most of the resources provided and to engage in its community of practice. The WASPI framework is an essential enabler for staff and organisations to provide the best service possible, through sharing information effectively and legally and I am pleased to endorse it.

**Julie James**

Leader of the House and Chief Whip  
August 2018

---



I am delighted to offer the continued support of the Information Commissioner to the WASPI programme and resources. Wales took a positive and proactive approach many years ago in developing WASPI, and I am pleased that my office has been able to contribute to updating the resources to reflect the new requirements of GDPR and the Data Protection Act 2018.

Sharing personal data appropriately, legally and securely is a vital component of effective public services. And yet I know from speaking and meeting with organisations that they face many cultural barriers within and outside their organisations to the safe and proportionate sharing of data. Clear guidance and commitments assist in meeting some of these cultural barriers head on.

One of my key aims as Information Commissioner is to increase public trust and organisational confidence in sharing data. WASPI helps to ensure that organisations in Wales plan their data sharing carefully, and provide the necessary accountability and transparency to their service users that will help build that trust and confidence.

The General Data Protection Regulation, and the Data Protection Act 2018 are a response to citizens' growing concerns about information rights, and control of their personal data. The new laws require additional accountability and transparency in data handling, and data controllers of all sizes must ensure that they have effective policies and procedures in place. WASPI will help organisations with those responsibilities in the context of data sharing. My office's website is also a good source of advice and guidance [www.ico.org.uk](http://www.ico.org.uk).

I look forward to hearing about the continued progress of WASPI.

**Elizabeth Denham**  
Information Commissioner  
August 2018

---

# Introduction and Purpose

## 1.1 Introduction

- 1.1.1 The Wales Accord on the Sharing of Personal Information (WASPI) is supported by the Welsh Government as the 'single' information sharing framework for Wales.
- 1.1.2 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.
- 1.1.3 This framework applies to all public sector organisations, third sector organisations and private organisations contracted to deliver a public service.
- 1.1.4 Adoption of the framework across Wales will help ensure compliance with common law and statutory requirements. It also helps organisations meet the considerations set out in the Information Commissioner's statutory 'Data Sharing Code of Practice' and legal requirements for accountability.
- 1.1.5 The Accord applies to personal identifiable information, which can include pseudonymised data.
- 1.1.6 The Accord identifies the commitments required by each organisation to enable sharing of personal information. Sign up and ownership is at the highest level.
- 1.1.7 The Accord's implementation adds significant value to the delivery of effective and efficient services that meet the needs of those receiving them.
- 1.1.8 The Accord is a statement of the principles and assurances that govern the activity of information sharing. It ensures that the rights of all those involved in the process are protected.
- 1.1.9 The conditions, obligations and requirements set out in this Accord and supporting documentation apply to all staff who handle and share personal data. This includes direct employees, agency workers, those with honorary contracts and others working on behalf of the partner organisations including agents and sub-contractors.
- 1.1.10 This Accord will be reviewed by the WASPI Management Board bi-annually, or as changes to legislation dictate.

## 1.2 Framework documentation

- 1.2.1 The Accord is supported by template agreements with a focus on the purposes and legal basis for sharing personal information between organisations. Completed agreements are intended for operational use and will document the 'what, when, why, how and who' of information sharing practices for specific, lawful purposes.
- 1.2.2 A range of supporting documentation has been developed to assist organisations in implementing the framework and is available on the WASPI website - [www.waspi.org](http://www.waspi.org)

## 1.3 Adoption of the Accord

- 1.3.1 Formal adoption of this Accord is the responsibility of the Chief Executive or Chief Officer of either a statutory body, private or third sector organisation.
- 1.3.2 Each signatory organisation agrees to support the adoption, dissemination and implementation, monitoring and review of the Accord and its requirements in accordance with its own internal and any other jointly agreed and authorised information governance standard and/or operational policies and procedures.
- 1.3.3 Each organisation will identify a "Designated Person" to take responsibility for ensuring the requirements of paragraph 1.3.2, above, are met. This should be each organisation's Data Protection Officer or, where the requirement for this role does not exist, an individual with an equivalent level of seniority.
- 1.3.4 The Designated Person must satisfy themselves that their organisation will work towards the principles and assurances set out in this Accord.
- 1.3.5 The 'Declaration of Acceptance and Participation' should be completed and signed by the Chief Executive, Chief Officer, or equivalent to confirm adoption of the Accord. A copy of the declaration is available on the WASPI website.

## 2.1 Introduction

2.1.1 This section outlines the principal commitments that each signatory organisation will make by adopting this Accord. When fully implemented these should ensure that the organisation's treatment of data subjects' information is compliant with relevant legislation and good practice. Each partner is responsible for complying with the 'Accountability' provisions of data protection law.

## 2.2 Data Subjects' Rights

2.2.1 Each organisation will allow data subjects to exercise their rights fairly and consistently, and in accordance with any specific legislative requirements, regulations or guidance.

2.2.2 Each organisation must have in place appropriate policies and procedures to facilitate both the protection, and the exercising, of these and other rights.

2.2.3 Each organisation must be clear, open and transparent with data subjects about the collection and use of their personal information, paying particular attention to the 'right to be informed'.

2.2.4 All data subjects have the right to expect that information about them will be protected, managed and processed with the appropriate degree of privacy and confidence.

## 2.3 Legal Basis for Sharing

2.3.1 Before sharing personal information, each organisation shall ensure an appropriate legal basis has been established and documented.

2.3.2 WASPI standard templates require this legal basis to be documented and organisations should consider the requirement to maintain a record of processing activities established by data protection legislation.

## 2.4 Staff and Others with Access to Information

2.4.1 Each organisation must have in place its own operational policies and procedures to facilitate the effective processing of personal information and support its staff to share information appropriately, safely and lawfully.

- 2.4.2 Staff contracts must contain appropriate confidentiality clauses detailing the possible consequences of unauthorised or inappropriate disclosure of personal information.
- 2.4.3 Each organisation must have in place disciplinary procedures to be invoked if a member of staff is found to have breached the confidentiality of an individual.
- 2.4.4 Each organisation must ensure that staff with access to personal information have the necessary level of security clearance.
- 2.4.5 Each organisation must ensure staff with access to personal information receive an appropriate level of training, advice and support. Consideration should be given to the category and nature of information to which staff have access and whether their role includes any specific requirements to access personal information.
- 2.4.6 Appropriate contractual, data processing and confidentiality agreements must be in place to underpin the processing of personal information by a third party / processor.

## 2.5 Records Management

- 2.5.1 Each organisation is responsible for the confidentiality, integrity and availability of the personal information it processes.
- 2.5.2 Each organisation will take reasonable steps to advise any other party known to have received or to be holding inaccurate personal information.
- 2.5.3 All participating organisations will 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.

## 2.6 Information Security and Risk Management

- 2.6.1 Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information it processes.
- 2.6.2 Care must be taken, with all aggregated, depersonalised and anonymised information, to ensure that it is not possible to identify individuals, e.g. in areas of low population density/low occurrence, as this would still be personal information.
- 2.6.3 In order to offer an appropriate level of protection to personal information, organisations must apply appropriate physical, organisational and technical security measures.
- 2.6.4 Before developing and implementing new systems or working practices that process personal information, each organisation must consider the impact on individuals' privacy. Data Protection Impact Assessments (DPIAs) should be undertaken where necessary.
- 2.6.5 It is accepted that organisations vary in size and complexity. The application of any relevant standards, processes and security measures should take this into account.

## 2.7 Complaints and Concerns

- 2.7.1 Any concerns or complaints received from individuals about the processing of their personal data will be dealt with promptly and in accordance with the internal complaints procedures of that partner organisation.
- 2.7.2 All partner organisations must put in place processes that allow concerns about non-compliance with this framework to be reported to the Designated Person.

# Annex 1 – Glossary of Terms

## Term

Controller

## Definition

Usually an organisation, but can also be an individual, that determines the purposes for which and the manner in which any personal information is, or will be, processed.

Controllers must ensure any processing of personal information for which they are responsible complies with relevant legislation including the GDPR, and Data Protection Act 2018.

DPIA (Data Protection Impact Assessment)

Data protection impact assessments, also referred to as Privacy Impact Assessments (PIAs), are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Data Protection Legislation

The General Data Protection Regulation (GDPR) provides Europe-wide principles and rights and is supplemented by the Data Protection Act 2018.

The Data Protection Act creates specific provisions, such as exemptions allowed by GDPR, and incorporates the provisions of EU Data Protection Directive 2016/680 – the Law Enforcement Directive.

Data subject

A 'data subject' is an identified or identifiable natural person. Organisations may refer to data subjects as service users, patients, clients, citizens, staff etc but for consistency, WASPI framework documentation refers to data subjects.

Personal information / 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.

Practitioner	An inclusive term to describe an employee, or other person who works for or on behalf of a partner organisation, who is involved in the care of or provision of services for the data subject. For example: police officer, health professional, social worker, volunteer etc.
Processors	Organisations that process personal data under Contract to, and according to instructions from, the Controller(s). It is a legal requirement for Controllers to set out in writing the purpose and extent to which Processors may process personal information and the expected measures required to protect that information.
Third sector	A term used to describe the range of organisations that are neither public nor private sector. It includes voluntary and community organisations, registered charities and other organisations such as associations, self-help groups, community groups, social enterprises, mutuals and co-operatives.