Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

DRAFT CONSULTATION

Wales Accord on the Sharing of Personal Information

Joint Controller Agreement
[Insert details here]

Version	[Insert details here]
Issue Date	[Insert date here]
Review Date	[Insert date here]

Template Version 6

Template developed in partnership with

BLAKE MORGAN

Further information on how a Joint Controller Agreement should be developed is contained within the

Guide on the Development of a Joint Controller Agreement

Further guidance may be sought from the WASPI Service at: www.waspi.gov.wales

Note: This page can be removed once the JCA development has commenced

DRAFT CONSU

Template developed in partnership with

BLAKE MORGAN

Where two or more Controllers jointly determine the purposes and means of processing Personal Data, they shall be Joint Controllers. Article 26(1) UK GDPR requires Joint Controllers to determine, in a transparent manner (often in writing) their respective responsibilities for compliance with Data Protection Legislation.

A Joint Controller Agreement (JCA) is intended to help practitioners understand what decisions have been made about the processing of Personal Data between a number of partners.

A JCA provides assurance that the partners have considered the requirements of Data Protection Legislation as Joint Controllers and that each have identified their roles and responsibilities.

Organisations who use this WASPI JCA template need to ensure that any completed JCA is legally binding from their own organisational requirements. WASPI provide a template agreement which can be used, but exclude all warranties and representations about the suitability of the document and exclude all liability in respect of the processing or contracts in place. The WASPI service will not provide any opinions on any proposed agreements, data protection advice should be sought from relevant organisation's Data Protection leads.

The template JCA was developed by WASPI in partnership with Blake Morgan LLP. This template JCA has been prepared solely for the benefit of WASPI only. Whilst other organisations may use this JCA template, neither WASPI nor Blake Morgan shall owe any duty of care to any other entities and all liability of WASPI and Blake Morgan LLP to all other entities is hereby excluded. Other entities are advised seek their own advice on the contents and use of this template.

This template is only appropriate for Joint Controller relationships. Other WASPI templates are available for other processing arrangements at: https://www.waspi.gov.wales/framework-documentation/templates-and-guidance/

DRAFT CONSU

Template developed in partnership with

BLAKE MORGAN

Contents

Part 1: Front Sheet		2
Part 2: Terms and Conditions		4
1	Introduction	6
2	Purpose	6
3	The Joint Controller Partner Organisations and Responsibilities	7
4	Commencement and Duration	7
5	Specific Organisational / Partner Obligations	7
6	Data breaches, complaints and investigations	8
7	Legislative / Statutory Powers	8
8	Data Protection Principles, Accountability and Demonstrating Data Protection Compliance	9
9	Data Subjects' Rights and Privacy Information	10
10	Information security	11
11	Data Retention and Deletion	12
12	International transfers of Personal Data	12
13	Governance and decision making	12
14	Variation	12
15	Termination	13
16	Liability	13
17	Dispute Resolution	13
18	General	14
19	Appendix A – Lawful basis/es	14
20	Appendix B – Governance and decision making	18
21	Appendix C – Signatories	19

DRAFT CONSULTATION

Part 1: Front Sheet

A. The Partners set out below have identified they are Joint Controllers for the purposes of Article 26 of the UK General Data Protection Regulation (UK GDPR).

B. This JCA is intended to help practitioners understand what decisions have been made about the processing of Shared Personal Data between the Partners below for the stated purpose(s).

C. It also provides assurance that the Partners have considered the requirements of Data Protection Legislation as Joint Controllers and that each have identified their roles and responsibilities for processing the Shared Personal Data jointly. This JCA sets out these requirements under Article 26 GDPR.

D. This Front Sheet and the Terms and Conditions at part 2 (together, the **JCA**) record the obligations of the Partners in respect of these processing activities.

E. Where there is a conflict between the provisions of this Front Sheet and the Terms and Conditions, then the provisions of this Front Sheet shall prevail.

A.	**Partners**	See Signatories in Appendix C
B.	**Agreement Administrators**	[To be completed]
C.	**Purpose**	[To be completed - please be as specific as possible, but make sure that you cover all intended purposes of sharing the Personal Data (e.g. details of the project/programme/services which requires sharing of Personal Data]
D.	**Authorised Users**	[To be completed - this is in relation to each Partner who is authorised to process the relevant Shared Personal Data for the purposes stated in such privacy notice]
E.	**Commencement Date**	[DD] day of [insert month] 202[X]
F.	**Duration of the Processing**	[To be completed - clearly set out the duration of the joint controller arrangements, including dates]
G.	**Categories of Personal Data**	[To be completed – provide the categories of information involved in the agreement, such as demographic data, health data, criminal offence information.]
H.	**Categories of Data Subjects**	[To be completed - Examples include: Patients, service users, staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers,

DRAFT CONSULTATION

		patients, students / pupils, members of the public, users of a particular website etc]
I.	**Legal Bases for Processing**	See Appendix A
J.	**Agreed Sharing Mechanisms**	[To be completed - provide details as to how data will be shared]
K.	**Security**	[To be completed - details of the security measures that the parties are to have in place]
L.	**Confidentiality Compliance**	[To be completed]
M.	**Review data / frequency**	[To be completed]
N.	**Governance**	See Appendix B.

DRAFT CONSULTATION

Part 2: Terms and Conditions

Term	Definition
Agreed Sharing Mechanism	Means the technical measures described in the Front Sheet, being the means by which the Partners shall transmit Shared Personal Data between each other.
Agreement Administrator	The individual appointed by the Partners to be responsible for administering this JCA for and on behalf of the Partners.
Authorised User	As set out in the Front Sheet.
Controller/s	Has the meaning given to it in the Data Protection Legislation.
Data Discloser	Means a Partner who makes available any Shared Personal Data to another Partner.
Data Protection Impact Assessment	Means, for each Partner, its completed Data Protection Impact Assessment (DPIA) as prepared by it in accordance with the Data Protection Legislation.
Data Protection Legislation	Means all applicable laws, regulations and regulatory rules which govern the processing of Personal Data and privacy including but not limited to (i) the Data Protection Act 2018 (ii) the UK GDPR (and to the extent it applies the EU GDPR) (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (iv) any subsequent legislation enacted and duly in force from time to time relating to the processing of Personal Data and (v) all guidance and / or codes of practice issued from time to time by the Information Commission or relevant government department, and any relevant rulings from time to time of the Information Commission or of the Courts of England and Wales relating to the processing of Personal Data.
Data Protection Officer	Certain categories of organisation, including any public body or authority (except courts in their judicial capacity) are required to designate a suitably qualified Data Protection Officer (DPO). The tasks of the DPO are set out in Article 39 of UK GDPR.
Data Subject	Shall have the meaning given to it in the Data Protection Legislation.
Law Enforcement Purposes	The purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (DPA 2018 Part 3, Chapter 1, Section 31).
Personal Data	Has the meaning given int the Data Protection Legislation.

PUBLIC CONSULTATION

Personal Data Breach	Has the meaning given to it in the UK GDPR and includes also any breach of Article 5(1)(f) (the integrity and confidentiality principle) of the UK GDPR.
Personal Data about criminal convictions, offences or related security measures	This includes Personal Data which relates to the alleged commission of offences by the Data Subject, or proceedings for an offence committed or alleged to have been committed by the Data Subject or the disposal of such proceedings, including sentencing. (DPA 2018 Section 11(2))
Practitioner	An inclusive term that refers to those involved in the care, education, welfare of Data Subjects; i.e. those who provide a public service.
Processing Personal Data	'Processing' means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' (UK GDPR Art 4(2))
Purpose	Means the purpose set out in the Front Sheet.
Record of Processing Activities or ROPA	A record maintained by a Partner as Controller containing the information set out in Article 30 UK GDPR.
Shared Personal Data	The Personal Data to be shared between the Partners under the terms of this JCA.
UK GDPR	As defined in section 3(10) of the Data Protection Act 2018
[Insert further terms as appropriate]	

DRAFT CONSULTATION

1 Introduction

1.1 This Joint Controller Agreement (**JCA**) is supplementary to the Wales Accord on the Sharing of Personal Information (**WASPI**) and has been agreed following consultation between the participating partner organisations.

1.2 This JCA provides assurance that the Partners have considered the requirements of the Data Protection Legislation as Joint Controllers and that each have **identified their roles and responsibilities** for processing Shared Personal Data jointly. The JCA sets out these requirements under Article 26 of the UK General Data Protection Regulation (UK GDPR).

1.3 It is intended that this JCA is to be read alongside any Data Protection Impact Assessment (DPIA) prepared by the Partners.

1.4 This JCA sets out the framework for the for the sharing and processing of Shared Personal Data for the Purpose. The JCA defines the principles and procedures that the Partners will adhere to and the responsibilities of each Partner as Joint Controllers in relation to the sharing and use of Shared Personal Data in the delivery of the Purpose.

1.5 All Partners have entered this JCA to demonstrate that data protection and privacy requirements have been considered, to set out how use of information meets the data protection principles, and how rights of Data Subjects are protected. All Partners agree to observe all the obligations set out in this JCA and to comply with the Data Protection Legislation.

1.6 This JCA does not replace any contractual arrangement as between the Partners or any requirements for data processing agreements or data sharing agreements with any third party suppliers of any goods and/or services to deliver the Purpose.

1.7 This JCA has been prepared solely for the benefit of WASPI only. WASPI provide a template agreement which can be used. WASPI and Blake Morgan exclude all warranties and representations about the suitability of the document and exclude all liability in respect of the processing or contracts in place and shall not owe no duty of care to any other entities. Other entities using this agreement are advised seek their own advice on the contents and use of this template.

2 Purpose

2.1 Personal Data is processed by and shared between the Partners for the purpose of set out in the Front Sheet only.

DRAFT CONSULTATION

3 The Joint Controller Partner Organisations and Responsibilities

3.1 The table below sets out the Partners to the JCA and the respective roles and responsibilities in relation to the joint controllership arrangement for the purposes described in this JCA.

	(A) Controller Organisations	(B) Owner / Point of contact	(C) Departments / Divisions / Teams	(D) Organisation's Role and Responsibilities / Activities
Party A	[Insert organisation name here]	[Insert JCA owner / point of contact – Specify roles not individual names]	[Insert departments / divisions]	
Party B	[Insert organisation name here]	[Insert JCA owner / point of contact – Specify roles not individual names]	[Insert departments / divisions]	
Party C	[Insert further rows as necessary]			

3.2 Where the Partners may be public authorities, they are designed as public authorities for the purposes of the UK GDPR.

3.3 The JCA owners / points of contact have overall responsibility for this JCA within their respective organisations and must therefore ensure the JCA is disseminated, understood and acted upon by relevant practitioners.

3.4 The owners / point of contact for each partner organisation will regularly monitor and review the use of this JCA to ensure information is shared effectively and appropriately.

3.5 Each partner organisation will nominate a signatory to sign the JCA at Appendix C. The signatory will be an appropriate person from the partner organisation who can sign on behalf of the organisation.

4 Commencement and Duration

4.1 This JCA shall commence on the Commencement Date and shall continue in force until brought to an end in accordance with clause 15 or until the termination or expiry of the Purpose.

5 Specific Organisational / Partner Obligations

5.1 Practitioners who share information in line with this JCA should make themselves aware of, and adhere to, their organisation's Information Governance and Records Management Procedures in particular the provisions that relate to collecting, processing and disclosing Personal Data.

5.2 Each Partner will not disclose or allow access to the Shared Personal Data to anyone other than the Partners without the prior written authorisation of the Data Discloser and always subject to compliance with relevant safeguards and Data Protection Legislation.

DRAFT CONSULTATION

5.3 Every reasonable step should be taken to ensure that inaccurate Shared Personal Data are erased or rectified without delay. Consideration must be given to advising partner organisations that they may have received inaccurate information. In circumstances where Partner's cannot be informed, advice should be taken from an Information Governance lead (or equivalent).

6 Data breaches, complaints and investigations

6.1 Each Partner will notify the other Partner who are or foreseeably may be affected or implicated as soon as reasonably possible if it becomes aware of any breach of this JCA, any breach of any of the Data Protection Legislation regarding the Shared Personal Data, any Personal Data Breach affecting any Shared Personal Data. Any Partner that gives such notification shall provide the other Partners as soon as reasonably possible with such information regarding such breach as may be reasonably requested by any of the other Partners.

6.2 Any breaches of security, confidentiality and other violations of this JCA must be reported in line with each Partner's incident reporting procedures. Specifically, this includes the reporting, management and notification of Personal Data Breaches between the Partners and should operate a shared procedure for such. Consideration should be given to sharing the outcome of any investigation, where appropriate, with other partners to the JCA.

6.3 The DPO of the Partner responsible for the breach will assess and consider whether the Personal Data Breach requires to be reported to the information Commission (ICO). A log of Personal Data Breaches will be maintained by the DPO of the responsible Partner.

6.4 Each Partner (the **"Originating Partner"**) will give written notice to the other Partners who are or foreseeably may be affected or implicated (the **"Relevant Partners"**), as soon as reasonably possible, if the Originating Partner or any of its Processors or Permitted Third Party Controllers receive(s) any request, complaint, notice, order or communication which relates directly or indirectly to the processing of any Shared Personal Data or to compliance with the Data Protection Legislation and, at the same time, will forward a copy of that request, complaint, notice, order or communication to all Relevant Partner. The Originating Partner and each of the Relevant Partners will co-operate with each other and give each other such information and assistance as any other such Partner may reasonably require in relation to that request, complaint, notice or communication to enable the other such Partners to respond to the same in accordance with any deadline and any requirement to provide information.

7 Legislative / Statutory Powers

Lawful basis

7.1 Before sharing or processing Shared Personal Data, the Partners must have identified a clear legal basis for doing so. The bases for lawful processing will depend on the individual purposes and will be assessed on a case-by-case basis. The bases for lawful processing under the UK GDPR Article 6 and conditions for processing under special category data under Article 9 will be identified and approved in DPIAs conducted prior to implementing activities that involve joint

DRAFT CONSULTATION

processing and information sharing (as applicable). The lawful basis/es will be set out in Appendix A.

7.2 The Partners will publish their bases for lawful processing and conditions for processing special category data within their privacy notices.

7.3 Partner's also need to ensure they consider the Data Protection Act 2018 ("**the Act**") and any additional requirements it places on the use of the legal bases set out in Articles 6, 9 and 10 of UK GDPR (see Part 2 of the Act) and processing for the 'law enforcement purposes' (see Part 3 of the Act). The ICO has guidance on this matter and queries about the relevance of any legal basis should be raised with an Information Governance lead.

Common Law Duty of Confidentiality

7.4 Relying on consent to process Shared Personal Data (under Article 6(1)(a) of the UK GDPR) as a lawful basis to process Personal Data should not be confused with consent under Common Law Duty of Confidentiality. The two are separate and should not be confused or merged.

7.5 The Partners agree that when introducing measures to enable joint working, that they must satisfy the requirements of the Common Law Duty of Confidentiality to Data Subjects.

7.6 The common law duty of confidentiality is the general position that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's agreement. Generally, the common law allows disclosure of confidential information only if the individual consents to its disclosure, it is required by law (e.g. by statute or by court order) or it is justified in the public interest.

7.7 The Partners will achieve this by addressing confidentiality requirements in the application of data protection by design and default and identifying the legal gateways to demonstrate how processing has considered and satisfied a duty of confidence.

8 Data Protection Principles, Accountability and Demonstrating Data Protection Compliance

8.1 The Partners have entered into this JCA to assist them with processing Shared Personal Data in accordance with the data processing principles set out in Article 5 of the UK GDPR which are, in summary that Shared Personal Data shall be:

8.1.1 processed lawfully, fairly and in a transparent manner;

8.1.2 collected for specified, explicit and legitimate purposes;

8.1.3 adequate, relevant and limited to what is necessary;

8.1.4 accurate and, where necessary, kept up to date;

8.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; and

8.1.6 processed in a manner that ensures appropriate security of the Personal Data.

8.2 Additionally, accountability is another key principles in Data Protection Legislation and Partners are responsible for complying with the legislation and must be able to

DRAFT CONSULTATION

demonstrate their compliance. Each Partner is responsible either solely or jointly for the following:

8.2.1 A single Data Protection Officer (DPO) is appointed for their central functions as Controllers.

8.2.2 Each Partner shall ensure that its polices, privacy notice(s) and Data Protection Impact Assessments (as applicable) take full account of Shared Personal Data and the processing under this JCA and made available to each Partner upon its request.

8.2.3 The Partner will collaborate to ensure that a data protection by design and default approach is applied when implementing a new project, process, system or new joint working practices. This may include ensuring a DPIA has been completed for uses of Personal Data and obtaining approval for completed DPIAs through established governance processes.

8.3 The Partners will establish:

8.3.1 A DPIA to identify the purpose and nature of processing activities as joint or sole Controllers, and the legal bases for processing and sharing Shared Personal Data, where the processing is likely to result in a high risk to the rights and freedoms of individuals, or where the Partners agree that a DPIA is required (or an assessment of high risk processing). The ICO's Data Sharing Code of Practice recommends undertaking a DPIA, even where it may not be mandatory.

8.3.2 Information Sharing Agreements where these are applicable to the Joint Controller arrangement.

8.3.3 Other appropriate written contracts with organisations, or a Partner that processes Personal Data on behalf of a Controller.

8.4 UK GDPR Article 30 requires organisations to maintain documentation of processing activities, referred to as Records of Processing Activities (**ROPA**). Each Partner will record their processing activities to include Joint Controller responsibilities where these apply, and the specific information required under this Article.

8.5 The Partners will ensure they have implemented appropriate security measures for the sharing and handling of Shared Personal Data. This is demonstrated through the completion of a due diligence process that will provide assurance that a secure system/process is in place.

9 Data Subjects' Rights and Privacy Information

9.1 Data Protection Legislation provides various individual rights for Data Subjects. Advice on how these rights should be met should be sought from each organisation's Information Governance representative, Data Protection Officer or equivalent. Specific guidance on these rights is available on the ICO's website; www.ico.org.uk

9.2 The following paragraphs refer to key rights associated with processing and sharing Personal Data.

9.3 Data Subjects should be informed how and why their Personal Data will be processed and who it is shared with (the Right to be Informed). The Partners will collaborate to ensure appropriate privacy information is provided to Data Subjects in

DRAFT CONSULTATION

a concise, transparent, and easily accessible form. Generally, online privacy notices are provided as the method of informing Data Subjects about the processing and sharing of their personal and special category data.

9.4 Each Partner shall comply with the exercise by Data Subjects of their rights under Data Protection Legislation in accordance with this JCA.

9.5 The Partner in receipt of the request to exercise the Data Subject rights shall primarily be responsible for responding to such requests within the applicable time period as defined in Article 12A UK GDPR and in compliance with the Data Protection Legislation.

9.6 The Partner each agree to assist as is reasonably required to enable the other Partners to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation. Each Partner will, on the request of any other Partner:

9.6.1 promptly inform the other Partners about the receipt of any Data Subject access request and any other Data Subject rights request under the Data Protection Legislation.

9.6.2 provide the other Partners with reasonable assistance in complying with any Data Subject access request.

9.7 There is an expectation that each Partner will work together to keep all other Partners informed of any complaints or requests for information received from Data Subjects or third parties. The Partners will also keep each other informed of any problems associated with the information sharing practices documented for the Purpose and there is an expectation that they will collaborate to develop and improve these practices.

10 Information security

10.1 Each Partner will take (and procure that its processors and other Controllers it may share Personal Data with will take) appropriate technical and organisational measures (as defined in the Data Protection Legislation) to prevent unauthorised or unlawful processing of the Personal Data or the accidental loss or destruction of, or damage to, the Personal Data. Such technical and organisational measures shall ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the Personal Data to be protected.

10.2 Each Partner shall implement any security measures specified in the Front Sheet and such other security measures as are at any time approved and agreed between the Partners. The Partner shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the duration of this JCA.

10.3 Each Partner must have an appropriate and adequate security framework.

10.4 The Partner will have in place policies and procedures to uphold the confidentiality, integrity and availability of Personal Data with specific reference to the retention, storage and disposal of records.

10.5 Each Partner shall ensure, within its own organisation, that there is no disclosure of Personal Data to any person (including the Partner's own staff who are not permitted

DRAFT CONSULTATION

by the Authorised Users, and including other Partners as well as third parties) where such disclosure would be in breach of any duty of confidence. Each Partner shall ensure that the Processing of the Shared Personal Data is only performed by that Partner's Authorised staff and that such Authorised staff have received appropriate training.

10.6 Each Partner carrying out the specific roles and responsibilities outlined in this JCA should be aware of, and adhere to, their organisation's information security policies and procedures.

10.7 All Partners must ensure adequate and appropriate training on the subjects of data protection and confidentiality is provided to all staff with access to Personal Data.

10.8 Each Partner shall only disclose the Shared Personal Data to other Partner solely via the Agreed Sharing Mechanisms set out in the Front Sheet.

11 Data Retention and Deletion

11.1 The Partners shall not retain or process Shared Personal Data for longer than is necessary to carry out the Purpose.

11.2 Notwithstanding clause 11.1, Partners shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable.

12 International transfers of Personal Data

12.1 The Partners will not as standard transfer the Shared Personal Data outside of the UK or European Economic Area for the purposes of the delivery of the Purpose.

13 Governance and decision making

13.1 The Partners shall set out the governance and decisions-making process in respect of this JCA in Appendix B.

13.2 Each Partner will comply with its obligations under the Freedom of Information Act 2000 (**FOIA**) and the Environmental Information Regulations 2004 (SI 2004/3391) (**EIRs**). Where the Partners may be public authorities, they are designed as public authorities for FOIA and EIR purposes.

13.3 Where a Partner receives a request for information under FOIA or EIRs, and such request relates to the Shared Personal Data, the requested Partner shall notify the other Partners.

14 Variation

14.1 All Partners may request a change to the existing JCA through written notification to the other Partners.

14.2 All proposed changes will be discussed between the Data Protection Officers (DPOs) of all Partners of this JCA. Any changes that are agreed and implemented between the Partners will be incorporated into this JCA at the next revision of this JCA (with any amendment of variation only coming into effect once the amended or varied JCA is signed by all Partners) and also reflected in respective DPIAs and privacy notices.

DRAFT CONSULTATION

14.3 External changes affecting the operational delivery responsibilities of the Partners will also necessitate the review and potential amendment of the JCA.

14.4 All Partners to this JCA are expected to make every effort to ensure that any changes to the JCA are implemented with minimal disruption.

15 Termination

15.1 This JCA shall automatically terminate upon the expiry or termination of the Purpose.

15.2 Any Partner may terminate its participation in this JCA at any time by serving no less than twenty (20) working day's written notice to the duly designated Agreement Administrator.

15.3 A Partner shall immediately cease to be a party to this JCA if they cease to be a member of the Purpose.

15.4 In the event that a Partner's membership of the JCA is terminated, an amended and updated version of this JCA will be drafted as soon as practicable and circulated to all other Partners by the duly designated Agreement Administrator.

15.5 Each Partner shall, on the termination of its membership of this JCA:

15.5.1 cease to store, access and otherwise Process the Shared Personal Data that was made available to it by any Data Discloser under or in connection with this JCA (and shall procure that its Processors shall cease to so disclose Shared Personal Data); and

15.5.2 cease to disclose Shared Personal Data under or in connection with this JCA (and shall procure that its Processors shall cease to so disclose Shared Personal Data).

15.5.3 remove reference to the JCA and the Shared Personal Data in any Privacy Notice under its control; and

15.5.4 remove the interfaces and other means by which the relevant Partner's electronic information processing systems are connected with the remaining Partners' electronic information processing systems (and each of them).

15.6 Data Subject rights or any statutory duties or obligations incurred under Data Protection Legislation by any Partner to this JCA and which survive the expiry or termination of this JCA will continue after expiry or termination.

16 Liability

16.1 Nothing in this JCA is intended to limit any Partner's liability in respect of the exercise of any of its statutory functions or its obligations to comply with Data Protection Legislation.

17 Dispute Resolution

17.1 If any Partner has any issues, concerns or complaints about the JCA, or any matter in this JCA, that Partner shall notify the other Partners and the Partners shall, acting in good faith, seek to resolve the issue by negotiations between themselves. If the issue cannot be resolved within 7 days, the matter shall be escalated to the nominated representative and the Data Protection Officer who shall advise on the appropriate course of action to take.

DRAFT CONSULTATION

17.2 Any disagreement between the Partners regarding the application of this JCA will normally be resolved at working level. If this is not possible, it may be referred through those responsible for the management of this JCA, up to and including the heads of the organisations (e.g., Chief Executive / Permanent Secretary) who will then jointly be responsible for ensuring a mutually satisfactory resolution.

17.3 If the dispute cannot be resolved by the above contacts in clause 17.2 within 14 days, they shall seek legal advice.

18 General

18.1 The Partners enter the JCA intending to honour all their obligations, including compliance with Article 26 UK GDPR and Section 58 Data Protection Act 2018 (DPA 2018), regarding requirements for Joint Controllers.

18.2 Nothing in this JCA is intended to, or will be deemed to, establish any agreement or joint venture between the Partners, constitute any Partner as the agent of the other Partner, nor authorise the Partners to make or enter any commitments for or on behalf of the other Partner.

18.3 The JCA will be governed by and construed in accordance with English and Welsh law (as it applies in Wales).

19 Appendix A – Lawful basis/es

Table 1 - Article 6 - Personal Data

Lawful basis	Check box / Notes
Consent – Art 6(1)(a)	☐ *[Care should be taken when relying on consent and consideration should be given to the ICO's guide to consent and the UK GDPR.* *If relying on consent, organisations must consider Article 7 of UK GDPR and be able to:* • *demonstrate that the Data Subject has consented to the processing of their data* • *evidence how the Data Subject can withhold and retract consent* • *add a copy of the consent form to the appendices]*
Contract – Art 6(1)(b)	☐ *[Organisations should be able to justify their reasoning as to why an ISP is suitable where there is (or there will be) a contract in place with the Data Subject. If appropriate, the nature of the contract and the parties involved should be noted.]*
Necessary for compliance with a legal obligation – Art 6(1)(c)	☐ *[Organisations must be able to identify the specific legal obligation that requires information to be shared and should include the details here – title of legislation and relevant section(s).]*
Protection of vital interests – Art 6(1)(d)	☐

DRAFT CONSULTATION

	[Explain why sharing information is necessary to protect vital interests of the individual or third party – i.e life or death situation.]
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☐ *[It is anticipated that many public service providers will rely on this provision to share Personal Data. You should specify the relevant task, function or power and identify its statutory or common law basis.]*
Processing is necessary for the purposes of a recognised legitimate interest – Art 6(1)(ea)	☐ *[Please explain where processing is necessary for purposes of a recognised legitimate interest and detail which condition listed in Annex 1 of the UK GDPR is met.]*
Legitimate Interest – Art 6(1)(f)	☐ *[Organisations should consider whether this lawful basis is appropriate and why Art 6(1)(e) is not more appropriate. Public authorities cannot rely on this lawful basis unless they are processing for a legitimate reason other than performing their tasks as a public authority. If this lawful basis does apply, you should outline how this lawful basis applies in line with the ICO's three-part test and guidance available on the ICO website.]*

Table 2 - Article 9 - Special Categories of Personal Data

Lawful basis	Checkbox / Notes
Explicit Consent – Art 9(2)(a)	☐ *[Care should be taken when relying on consent and consideration should be given to the ICO's guide to consent and the UK GDPR.]*
Employment and social security and social protection law – Art 9(2)(b)	☐ *[You should specify the relevant task, function or power and identify its statutory or common law basis. See DPA 2018 Section 10(2).* *This lawful basis also requires an Appropriate Policy Document, each organisation should meet this requirement prior to sharing.]*
Vital interests of the Data Subject or a third party where they are incapable of giving consent – Art 9(2)(c)	☐ *[Explain why sharing information is necessary to protect vital interests – i.e life or death situation.]*
Legitimate Activities – Art 9(2)(d)	☐ *[This lawful basis should only be relied upon by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and the processing relates solely to members, former members, persons who have regular contact with it and the Personal Data is not disclosed outside of the body without consent of the Data Subjects.]*
Manifestly made public by the Data Subject – Art 9(2)(e)	
Establishment, exercise or defence of legal claims or where courts are	☐

DRAFT CONSULTATION

acting in their judicial capacity – Art 9(2)(f)	
Necessary for reasons of substantial public interest - Art 9(2)(g)	☐ UK GDPR Art 9(2)(g) requires a basis in UK law, which is provided by Section 10(3) of the Data Protection Act 2018. This in turn refers to the need to meet a relevant condition in Part 2 of Schedule 1 of the DPA 2018. The relevant condition is: *[Detail which condition in Part 2 of Schedule 1 is relied upon, copying in the text from the Act and adding further explanation where required.* *Most of these Schedule 1 conditions also require an Appropriate Policy Document, each organisation should meet this requirement prior to sharing.]*
Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)	☐ *[Where relying on this lawful basis, you should ensure that the processing of Personal Data is carried out by or under the responsibility of a health professional or social work professional or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law. See DPA 2018 Section 11(1).]*
Public health - Art 9(2)(i)	☐ *[Where relying on this lawful basis, you should ensure that the processing is necessary for reasons of public interest in the area of public health (such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices).* *The processing should also be carried out by or under the responsibility of a health professional or by or under a person who in the circumstances owe a duty of confidentiality under an enactment or rule of law. See DPA 2018 Section 10(2).]*
Research – Art 9(2)(j)	☐ *[Explain which purpose is being relied upon (archiving, scientific, historical or statistical purposes).* *You should ensure the processing is in the public interest.]*

Table 3 - Article 10 - Personal Data about criminal convictions, offences or related security measures

The sharing of Personal Data relating to criminal convictions, offences or related security measures	*[You should have already selected a lawful basis for processing under Article 6.]* Processing is: ☐ Carried out under the control of an official authority / competent authority. *[if ticked, move to table 4.]* and/or ☐ Meets a relevant condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018. The relevant condition is:

DRAFT CONSULTATION

	[Detail which condition under Part 1, 2 or 3 of Schedule 1 is being relied upon, copying in the text and adding further explanation where required.]

Table 4 - Competent authorities for Law Enforcement Purposes

Processing **Personal Data** for law enforcement purposes	The Data Protection Act 2018, Part 3, Chapter 2, Section 35(2) outlines the lawful basis for sharing Personal Data for law enforcement purposes. The processing is based on law and (select one): ☐ 35(2)(a) The Data Subject has given consent. or ☐ 35(2)(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority.
Sensitive processing / **processing Special Categories of Personal Data** for law enforcement purposes	*[You should have already selected either 35(2)(a) or 35(2)(b) above.* *These lawful basis also requires an Appropriate Policy Document, each organisation should meet this requirement prior to sharing.]* The Data Protection Act 2018, Part 3, Chapter 2, Section 35(3) outlines the lawful basis for sharing sensitive / Special categories of data for law enforcement purposes. The lawful basis is (select one): ☐ 35(4) The Data Subject has given consent or ☐ 35(5) The processing is strictly necessary for the law enforcement purpose, and Meets a relevant condition in Schedule 8. The relevant condition is: *[Detail which condition under Schedule 8 is being relied upon, copying in the text and adding further explanation where required.]*

DRAFT CONSULTATION

20 Appendix B – Governance and decision making

[e.g, this may include operational data protection governance arrangements or applicable memorandum of understanding]

DRAFT CONSULTATION

21 Appendix C – Signatories

By signing below, partners are confirming they agree with the content of the JCA. In the context of processing and sharing Personal Data, signing the JCA is one way to demonstrate accountability with the principles set out in Article 5 of UK GDPR.

The signatory will be an appropriate person with authority to sign the JCA on behalf of the organisation.

Partner Organisation		**Partner Organisation**	
Name		**Name**	
Position		**Position**	
Date		**Date**	
Signature		**Signature**	

Partner Organisation		**Partner Organisation**	
Name		**Name**	
Position		**Position**	
Date		**Date**	
Signature		**Signature**	

[Insert additional tables if required]

DRAFT CONSULTATION