Schedule 7 - Data Sharing Agreement between Controllers

entered into between

(1) [Council]

AND

(2) [insert name]

Dated [ ]

Contents

Clauses

1	Interpretation	3
2	Purpose	5
3	Compliance with Data Protection Legislation	5
4	Shared Personal Data	5
5	Lawful, Fair and Transparent Processing	6
6	Data Subjects' Rights	6
7	Data Retention and Deletion	7
8	Transfers of Shared Personal Data Outside of the UK	7
9	Security and Training	8
10	Personal Data Breaches and Reporting Procedures	8
11	Review of Agreement	9
12	Direct Marketing	9
13	Resolution of Disputes with Data Subjects or Regulatory Authorities	9
14	Warranties and Indemnity	9
15	Limitation of Liability	10
16	Allocation of Cost	10
17	Termination	10
18	Third Party Rights	11
19	Rights and Remedies	11
20	Notice	11
21	Variation	11
22	Waiver	11
23	Changes to Data Protection Legislation	11
24	No Partnership or Agency	11
25	Entire Agreement	12
26	Governing Law and Jurisdiction	12

Schedule 1 13

Schedule 2 16

Schedule 3 20

Schedule 4 21

Schedule 5 22

Schedule 6 23

Schedule 7 24

Schedule 8 25

Schedule 9 26

Schedule 10 27

Schedule 11 28

This Agreement is made the day of 20

Between:

(1) [Council], of [address] (the **Council**); and

(2) [INSERT] a company registered in [INSERT] with company number [INSERT] whose registered office address is at [INSERT] (the **Partner**).

Background:

(A) [Insert background information about the sharing arrangement.]

(B) The parties have agreed to share personal data for the Agreed Purpose on the terms of this Agreement and for the benefits as set out in this Agreement.

(C) This Agreement is free-standing and does not incorporate terms established by the parties under any separate arrangements.

1 Interpretation

The following definitions and rules of interpretation apply in this Agreement:

Agreed Purpose	the purpose(s) for which the parties are entitled to use the Shared Personal Data, as set out in Schedule 2.
Agreement	this data sharing agreement including the schedules.
Business Day	a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.
Commencement Date	As per the Contract.
Contract	Overarching Contract for the Adult Social Care and Support Services incorporated by reference into all individual spot orders.
Criminal Offence Data	personal data relating to criminal convictions and offences or related security measures to be read in accordance with section 11(2) of the DPA 2018.
Data Discloser and Data Receiver	have the meaning given to them in clause 2.1 below.
Data Protection Legislation	all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended, and the guidance and codes of practice issued by the Information Commissioner or any relevant data protection or supervisory authority and applicable to a party.

Data Subject	an identified or identifiable natural person to whom the Shared Personal Data relates.
Deletion Procedure	the deletion procedure agreed by the parties and set out at Schedule 6 of this Agreement.
Insolvency Event	if a party makes any voluntary arrangement with its creditors, enters administration or goes into liquidation; if a security holder takes possession or a receiver or administrative receiver is appointed; if anything analogous to the foregoing occurs in any jurisdiction; or if that party ceases to do business.
Permitted Recipient	a director, employee or professional advisor of each respective party or an agent or contractor used by that party in the fulfilment of the Agreed Purpose(s) who has a legitimate need to receive and process Personal Data for the Agreed Purpose(s).
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.
Regulatory Authority	the Information Commissioner's Office or where applicable, other relevant supervisory authority.
Shared Personal Data	the personal data (including special categories of personal data) to be shared between the parties under this Agreement, as set out in Schedule 1.
SPoC	Single Point of Contact as defined in clause 2.4
Subject Access Request	a request from a Data Subject to exercise his or her right of access to Shared Personal Data under the Data Protection Legislation.
Term	As per the Contract.
Third Country/Countries	all countries outside of the scope of the Data Protection Legislation, excluding those countries which the UK government has approved under the applicable Data Protection Legislation as providing adequate protection.
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.1 **Controller, Information Commissioner, Joint Controller, Personal Data, process, Processor, Special Categories of Data** and **appropriate technical and**

organisational measures shall have the meanings given to them in the Data Protection Legislation.

1.2 Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.

1.3 Any phrase introduced by the terms include, including or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

1.4 The Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to his agreement includes the Schedules.

1.5 In the case of any ambiguity between any provision contained in the body of this Agreement and any provision contained in the Schedules, the provision in the body of this Agreement shall take precedence.

1.6 A reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended, extended or re-enacted from time to time.

2 Purpose

2.1 This Agreement sets out the framework for the sharing of Personal Data when one Controller (the **Data Discloser**) discloses Personal Data to another Controller (the **Data Receiver**) between the parties as Controllers. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other in respect of the Shared Personal Data.

2.2 The parties consider this data sharing necessary as the parties will be sharing Personal Data, including the individual's care needs. The aim of the data sharing initiative is to deliver a social care service. It will serve to benefit individuals by enabling individuals to receive the care they need.

2.3 The parties agree to only process Shared Personal Data as described and set out in Schedule 1 for the reasons set out in Schedule 2.

2.4 Each party shall nominate a single point of contact (**SPoC**) who will work together to reach agreement with regard to any issues arising from this Agreement and to actively improve the effectiveness of the Agreement going forward. The SPoC for each party is set out at Schedule 3.

3 Compliance with Data Protection Legislation

3.1 Each party must ensure compliance with applicable Data Protection Legislation at all times during the Term.

3.2 Each party has such valid registrations and/or has paid applicable fees as are required by the Information Commissioner during the Term unless an exemption applies.

4 Shared Personal Data

4.1 The Parties agree to only process Shared Personal Data for the Agreed Purpose.

4.2 The parties will provide to each other the Shared Personal Data at the times, frequencies and in the format set out at Schedule 4 or as otherwise agreed in writing between the parties.

4.3 Criminal Offence Data will be shared between the parties during the Term.

5 Lawful, Fair and Transparent Processing

5.1 The parties shall not process Shared Personal Data in a way that is not compatible with the Agreed Purpose. Each party shall ensure that it processes the Shared Personal Data fairly and lawfully during the Term. The lawful bases (and conditions or exceptions for processing of any categories of Personal Data or Criminal Offence Data) and the legal power for data sharing are set out in Schedule 2.

5.2 **Privacy information** The Data Discloser shall, in respect of Shared Personal Data, ensure that it provides clear and sufficient information to the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for such purposes and such other information as is required by Article 13 of the UK GDPR including whether Personal data will be transferred to a third party and if so sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer.

5.3 The Data Receiver undertakes to inform the Data Subjects, in accordance with UK GDPR, of the purposes for which it will process their personal data, the legal basis for those purposes and such other information as is required by Article 14 including whether Personal data will be transferred to a third party and if so sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer. - Not used.

5.4 If, for any reason, one party reasonably considers that the data sharing under this Agreement is not lawful, fair or transparent, the SPoC of that first party shall immediately contact the SPoC of the other party or parties to notify them of that concern and consider what action, including suspending any future data sharing, needs to be taken.

5.5 **Data Quality** Before the Commencement Date, the Data Discloser shall ensure that the Shared Personal Data is accurate and is not irrelevant or excessive with regard to the Agreed Purposes.

5.6 The parties agree that they shall record all Shared Personal Data using compatible databases and the data transfer methods as set out in Schedule 5 or as otherwise agreed in writing between the parties.

6 Data Subjects' Rights

6.1 The SPoC for each party is responsible for maintaining a record of individual requests from Data Subjects to exercise their rights under the Data Protection Legislation, including Subject Access Requests, requests for deletion, restriction, rectification, portability, objections and rights in relation to automated decision making.

6.2 In the event that a Data Subject makes an information rights request under sections 15-22 of the UK GDPR (including but not limited to a Subject Access Request) the party which holds the Shared Personal Data (and/or other applicable Personal Data) shall be responsible for responding to such request within the time frames specified within the Data Protection Legislation. The other party shall provide all reasonable assistance to enable compliance with such request within five (5) Business Days of being notified of that request.

1.3 Not Used.

6.4 Each party shall bear its own costs of complying with this clause 6 unless agreed otherwise in writing between the Council and the Partner.

6.5 In the event that the Partner collects Personal Data directly from a Data Subject, they shall provide the Data Subject with the information set out at Schedule 10, save where the Data Subject already has that information.

1.6 In the event that the one party obtains Personal Data from the other party, the party receiving the Personal Data shall provide the Data Subject with the information set out at Schedule 11, save where:

6.1.1 the Data Subject already has the information;

6.1.2 the provision of such information proves impossible or would involve a disproportionate effort; and/or

6.1.3 the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by the European Union or under English law, including a statutory obligation of secrecy.

7 Data Retention and Deletion

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

7.2 Notwithstanding clause 7.1, each party may continue to retain Shared Personal Data in accordance with any applicable statutory or professional retention periods.

7.3 The Data Receiver shall ensure that all Shared Personal Data is returned to the Data Discloser party or destroyed in accordance with the agreed Deletion Procedure:

7.3.1 on termination or expiry of this Agreement; or

7.3.2 once processing of the Shared Personal Data is no longer necessary for the Agreed Purposes.

7.4 Following the deletion of the Shared Personal Data in accordance with clause 7.3, each party shall notify the other that the Shared Personal Data in question has been deleted in accordance with the Deletion Procedure.

8 Transfers of Shared Personal Data Outside of the UK

8.1 For the purposes of this clause, transfers of Personal Data shall mean any sharing of Personal Data by the Data Receiver outside of the UK, and shall include the following:

8.1.1 subcontracting the processing of Shared Personal Data;

8.1.2 sharing the data within the Data Receiver's own organisation, where such organisation is located in part outside of the UK; and

8.1.3 granting a third-party Controller access to the Shared Personal Data.

8.2 If the Data Receiver appoints a third-party Processor to process the Shared Personal Data it shall comply with Article 28 UK GDPR and shall remain liable to the Data Discloser for the acts and omissions of the Processor.

8.3 The Data Receiver may not transfer Shared Personal Data outside the UK, nor shall it transfer Shared Personal Data to a third party located outside the UK unless the party receiving such data:

8.3.1 Complies with the provisions of Article 26 of the UK GDPR (in the event the third party is a Joint Controller); and

8.3.2 Ensures that either:

8.3.2.1 the transfer is to a country approved under the Data Protection Legislation as providing adequate protection;

8.3.2.2 there are appropriate safeguards or binding corporate rules in place pursuant to Data Protection Legislation,

8.3.2.3 the transferor otherwise complies with its obligations under the applicable Data Protection Legislation by proving an adequate level of protection to any Personal Data that is transferred; or

8.3.2.4 a derogation for specific situations in the Data Protection Legislation applies to the transfer, and the transferor notifies the Data Discloser of this in writing in advance of the transfer.

9 Security and Training

9.1 The Data Discloser shall only provide the Shared Personal Data to the Data Receiver by using secure methods. These may be agreed and set out in Schedule 9.

9.2 Having regard to the state of technological development and the cost of implementing such measures as appropriate at the Commencement Date, each party shall have and maintain in place throughout the Term appropriate technical and organisational measures as set out in Schedule 7 in order to:

9.2.1 prevent:

9.2.1.1 unauthorised or unlawful processing of the Shared Personal Data; and

9.2.1.2 the accidental loss or destruction of, or damage to, the Shared Personal Data; and

9.2.2 ensure a level of security appropriate to:

9.2.2.1 the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and

9.2.2.2 the nature of the Shared Personal Data to be protected.

9.3 Each party shall ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures set out in Schedule 7 and the Data Protection Legislation.

9.4 The level, content and regularity of training referred to in clause 9.3 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and processing of the Shared Personal Data and to the nature of the Shared Personal Data handled by the relevant staff members.

9.5 Each party shall ensure that only Permitted Recipients have access to the Shared Personal Data and shall ensure the reliability of all such Permitted Recipients.

10 Personal Data Breaches and Reporting Procedures

10.1 The Partner shall notify any loss of the Shared Personal Data, and any Data Security Breach, to the Council's SPoC as soon as possible and in any event within 24 hours after becoming aware of the breach. The SPoCs shall work together to consider the action required in order to resolve the issue in accordance with the applicable Data Protection Legislation.

10.2 Each party shall provide reasonable assistance as is necessary to the other to facilitate the handling by the other party of any Data Security Breach in an expeditious and compliant manner.

11 Review of Agreement

11.1 If the Data Receiver wishes to request Shared Personal Data from the Data Discloser under this Agreement, the Data Receiver shall complete and submit to the Data Discloser a data sharing request form in the form set out at Schedule 8. The Data Discloser shall then complete and submit a data sharing decision form as set out in Schedule 9. – NOT USED.

11.2 The parties shall review the effectiveness of this data sharing initiative and Agreement every 12 months and upon the addition and removal of a party, having consideration to the aims and purposes set out in this Agreement and to the Agreed Purpose. The parties shall continue, amend or terminate this Agreement depending on the outcome of this review.

11.3 The review of the effectiveness of the data sharing initiative and Agreement will involve at least the following:

11.3.1 assessing whether the purposes for which the Shared Personal Data is being processed still align with the Agreed Purpose;

11.3.2 assessing whether the Shared Personal Data is still as listed in Schedule 1 to this Agreement or whether the scope of the Shared Personal Data needs to be amended;

11.3.3 assessing whether the legal frameworks governing data quality, retention and Data Subjects' rights are being complied with; and

11.3.4 assessing whether Data Security Breaches involving the Shared Personal Data have been handled in accordance with this Agreement and the applicable Data Protection Legislation.

12 Direct Marketing

12.1 If the Data Receiver processes the Shared Personal Data for the purposes of direct marketing, the Data Receiver shall ensure that effective procedures are in place to allow the Data Subjects to opt-out from having their Shared Personal Data used for such direct marketing purposes in accordance with the Data Protection Legislation.– NOT USED.

13 Resolution of Disputes with Data Subjects or Regulatory Authorities

13.1 In the event of a dispute or claim brought by a Data Subject or a relevant Regulatory Authority concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

13.2 The Partner agrees to respond to any generally available non-binding mediation procedure initiated by a Data Subject or Regulatory Authority and to consider participating in any other dispute resolution proceedings developed for data protection disputes as requested by the Council.

13.3 Each party shall abide by a decision of a competent court of the UK or of the Information Commissioner's Office which is final and against which no further appeal is possible.

14 Warranties and Indemnity

14.1 The Partner warrants and undertakes that it will:

14.1.1 process the Shared Personal Data in compliance with all applicable Data Protection Legislation;

14.1.2 make a copy of this Agreement available upon request to the Data Subjects who are third party beneficiaries;

14.1.3 respond within a reasonable time and as far as reasonably possible to enquiries from any relevant Regulatory Authority in relation to the Shared Personal Data;

14.1.4 where applicable, maintain registration with all relevant Regulatory Authorities to enable the Partner to process all Shared Personal Data for the Agreed Purpose;

14.1.5 take all appropriate steps to ensure compliance with the security measures set out at clause 9 above.

14.2 Except as expressly stated in this Agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.

14.3 The Partner undertakes to indemnify the Council and hold the Council harmless from any costs, charge, damages, expense or loss incurred or suffered by the Council as a result of the breach by the Partner of any of the provisions of this Agreement.

14.4 For the avoidance of doubt, the indemnity at clause 14.3 applies without limitation to any cost, charge, damage expense or loss suffered by the Council in relation to any investigation, audit and/or enforcement action undertaken by the Regulatory Authority in relation to the Partner's breach of this Agreement.

15 Limitation of Liability

15.1 Neither party excludes or limits liability to the other party for:

15.1.1 fraud or fraudulent misrepresentation;

15.1.2 death or personal injury caused by negligence; or

15.1.3 any matter for which it would be unlawful for the parties to exclude or limit liability.

15.2 Each Party accepts responsibility for any costs, charge, damages, expense or loss which arises following its own breach of this Agreement.

16 Allocation of Cost

16.1 Except as expressly set out in this Agreement, each party shall perform its obligations under this Agreement at its own cost.

17 Termination

17.1 The Council shall be entitled to terminate this Agreement in the event that the Partner:

17.1.1 commits a material breach of any of the terms of this Agreement, which breach is irremediable or, if remediable, has not been remedied within thirty (30) days of receipt by the Partner of a notice in writing from the Council requiring the Partner to remedy it; or

17.1.2 suffers an Insolvency Event.

17.2 The parties are entitled to terminate this Agreement in the event that:

17.2.1 any underlying agreement to which this Agreement relates, is terminated or expires; or

17.2.2 where agreed by the parties in accordance with clause 11.2.

18 Third Party Rights

18.1 Other than as expressly set out in this Agreement, a person who is not a party to this Agreement is not entitled to enforce any of its terms, whether under the Contracts (Rights of Third Parties) Act 1999 or otherwise. If a person who is not a party to this Agreement is stated to have the right to enforce any of its terms, the parties may rescind or vary this Agreement without the consent of that person.

19 Rights and Remedies

19.1 The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

20 Notice

20.1 Any notice given to a party under or in connection with this Agreement shall be in writing, addressed to that party's SPoC and shall be delivered by hand or by recorded delivery at the address for the SPoC notified in Schedule 3.

20.2 Any notice shall be deemed to have been received:

20.2.1 if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address; and

20.2.2 if sent by pre-paid first-class post or other next working day delivery service, at 9:00am on the second Business Day after posting or at the time recorded by the delivery service.

21 Variation

21.1 No variation of this Agreement shall be effective unless it is in writing and signed by the duly authorised representatives of each of the parties.

22 Waiver

22.1 No failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

23 Changes to Data Protection Legislation

23.1 If the Data Protection Legislation applicable to either party changes in a way such that this Agreement is no longer adequate for the purposes of governing lawful data sharing, the parties agree that the SPoC for each party will negotiate in good faith to review the Agreement in light of the changes and to make any amendments required to enable this Agreement to be adequate for those purposes.

24 No Partnership or Agency

24.1 Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

25 Entire Agreement

25.1 This Agreement constitutes the entire agreement and understanding between the parties with respect to the subject matter of this Agreement and the terms of this Agreement shall supersede any previous agreements.

26 Governing Law and Jurisdiction

26.1 This Agreement shall be governed by and construed in accordance with the law of England and Wales and any dispute arising under or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of England and Wales, to which each of the parties irrevocably submits.

In witness whereof this Agreement has been signed by the parties or their duly authorised representatives on the date written at the beginning of this Agreement.

Signed by for and on behalf of **[Council]**	)))

Signed by for and on behalf of **[Partner]**	)))

Schedule 1

Shared Personal Data

Please:

- indicate which categories of Personal data apply to the data being processed by the Partner
- add further categories of Personal data under the column 'Other', where applicable

Type of personal data	Indicate where applicable
Name	**X**
Contact details	**X**
Bank details	**X**
Identification number	**X**
Location data	**X**
Online identifier (email / IP address)	**X**
Other (Please insert details) Date of birth Gender Marital status Next of Kin	 **X** **X** **X** **X**

1.2 Special Category Data[1]

Please indicate which types of data will be processed by the Partner:

Type of Special Category Data	Indicate where applicable
Race (data which identifies the race of the Data Subject, including the Data Subject's image)	**X**
Ethnic origin (data which identifies the ethnic background of the individual, including the Data Subject's image)	**X**
Political opinions (data which identifies the political opinion of the Data Subject)	
Religion (data which lists the religious beliefs of the Data Subject)	**X**
Trade Union Membership (data which lists the TU membership of the Data Subject)	
Genetics (data relating to the genetics of the Data Subject)	
Biometrics (Biometric data, where used for ID purposes)	
Health (records relating to a Data Subject's physical or mental health)	**X**

[1] Unlike 'personal data', Special Category Data is an exhaustive list of types of data, as listed in full here. For more information see: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Sexuality or sex life	**X**

Criminal Offence Data	Indicate where applicable
Data relating to **allegations** against the Data Subject	X
Data relating to **proceedings** against/involving the Data Subject	X
Data relating to **convictions** against the Data Subject	X

1.3 Whose data is shared: categories of Data Subjects

Categories of Data Subjects	Indicate where applicable
Council service-users	X
Council service-users' next of kin	X
Council employees	X
Council employees' next of kin	
Other (Please insert details)	

1.4 What data processing takes place?
Please indicate processing operations relevant to the Partner's processing of Shared Personal Data:

Processing Operations	Indicate where applicable
Using data provided by the Council	X
Collecting new data from Data Subjects	X
Transforming data by adding new data collected from service users to data provided by the Council	X
Sharing data with anyone other than the Council	X
Erasure or destruction of personal data	X
Other (Please insert details)	

1.5 **Where will the Partner's processing of the Shared Personal Data take place?**

Location of processing operations	Indicate where applicable
UK only	X
To a Third Country [2]	X
Outside both UK and any Third Country	

Schedule 2

Why the Parties use the Shared Personal Data, and the reason ("lawful basis") that they do so

As Controller, the Partner is legally required to explain:

- ✓ why it will use the data which is being shared under the terms of this agreement,
- ✓ their reason, or 'lawful basis', for doing so under the UK GDPR.

This information is set out in this Schedule 2. Please complete **Section 1** and then **Section 2 *OR* 3,** (as relevant) and **Section 4.**

Section 1:

Please indicate whether (A) or (B) applies to the Partner's sharing and processing of data shared under this Agreement.

The Council and the Partner shall share and process the Shared Personal Data:

X	(A)	For the **same purpose(s)** which the parties determine **jointly**	If this applies, please complete **Sections 2 and 4** below only
	(B)	**For different purpose(s)** which the parties determine **independently**	If this applies, please complete **Section 3 and 4** below only

Section 2:

If you indicated (A) at Section 1 above, please complete this Section 2 and Section 4. You <u>need not</u> complete Section 3 below.

Please list the shared purposes for which the data is used by the Council and Partner below **("the Agreed Purpose")**

The provision of adult care and support services.

[2] The EEA comprises: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden Norway, Lichtenstein and Iceland.

For a list of the countries and territories given a finding of adequacy as of January 2022 see the ICO website

Section 3:

If you indicated (B) at Section 1 above, please complete Section 3 and Section 4. You <u>need not</u> complete Section 2.

Please list the purposes for which the data is used by the Partner **("the Agreed Purpose")**

Section 4:

Why do you process the data? Please indicate which lawful basis/bases apply

Legal basis:	**Indicate if relied upon:**	**Details:**
Processing necessary for performance of a task carried out in the public interest	Yes	
Processing necessary for compliance with a legal obligation	Yes	
Processing necessary for performance of a contract with Data Subject or to take steps at request of Data Subject prior to entering into a contract		
Processing necessary for the purposes of the legitimate interests of the Council or the Partner and those interests are not overridden by the privacy rights and interests of the individual		
Data Subject has consented to processing		
Processing necessary to protect vital interests of Data Subject		

Where special category data is being processed, please specify two bases in relation to that data:

1. Lawful basis from the list above…….
2. Additional basis from the table below: …….

Additional basis:	Indicate if this additional basis is relied upon	Additional comments
Substantial Public Interest	**Yes**	
27 Where Substantial Public Interest is the appropriate lawful basis, an additional 'public interest condition' should be identified. Please indicate which is most applicable:	Statutory and government purposes Administration of justice and parliamentary purposes Equality of opportunity or treatment Racial and ethnic diversity at senior levels Preventing or detecting unlawful acts Protecting the public Regulatory requirements Journalism, academia, art and literature Preventing fraud Suspicion of terrorist financing or money laundering Support for individuals with a particular disability or medical condition Counselling Safeguarding of children and individuals at risk Safeguarding of economic well-being of certain individuals Insurance Occupational pensions Political parties Elected representatives responding to requests Disclosure to elected representatives Informing elected representatives about prisoners Publication of legal judgments Anti-doping in sport Standards of behaviour in sport	
Establishment, exercise or defence of legal claims		
Provision of health or social care	**Yes**	
Employment, social security and social protection: legal rights and obligations		
Not for profit bodies		
Manifestly made public by the Data Subject		
Archiving in the public interest, research or statistics		
Public health		

Additional basis:	Indicate if this additional basis is relied upon	Additional comments
Substantial Public Interest	**Yes**	
27 Where Substantial Public Interest is the appropriate lawful basis, an additional 'public interest condition' should be identified. Please indicate which is most applicable:	Statutory and government purposes Administration of justice and parliamentary purposes Equality of opportunity or treatment Racial and ethnic diversity at senior levels Preventing or detecting unlawful acts Protecting the public Regulatory requirements Journalism, academia, art and literature Preventing fraud Suspicion of terrorist financing or money laundering Support for individuals with a particular disability or medical condition Counselling Safeguarding of children and individuals at risk Safeguarding of economic well-being of certain individuals Insurance Occupational pensions Political parties Elected representatives responding to requests Disclosure to elected representatives Informing elected representatives about prisoners Publication of legal judgments Anti-doping in sport Standards of behaviour in sport	
Establishment, exercise or defence of legal claims		
Provision of health or social care	**Yes**	
Explicit Consent of Data Subject		

If criminal data is being processed, please contact Legal:

such processing is restricted.

Schedule 3

Single Points of Contact - NOT USED

Schedule 4 – NOT USED

Schedule 5 – NOT USED

Schedule 6 – NOT USED

Schedule 7

Security Measures

1. In advance of the Commencement Date and for the duration of the Term, the Supplier shall ensure that:

   1.1. the Supplier is certified to ISO/IEC 27001:2013 and/or able to demonstrate that its policies, procedures and information risk management processes are of a standard which is equivalent to that certification, save where the parties agree that the risks associated with the Supplier's data processing are low and therefore a proportionate adjustment of the policies, procedures and information risk management processes may be agreed by the Council on a case-by-case basis and in advance of the signing of this Agreement.

   1.2. the Supplier holds a Cyber Essentials Plus certificate or is able to demonstrate an equivalent commitment to cyber security by undergoing annual independent penetration tests.

2. Where appropriate, the Supplier shall be able to ensure that the Supplier, and any third parties that the Supplier relies upon, is certified to the appropriate level of the Payment Card Industry Data Security Standard.

3. The Supplier shall adhere to the National Cyber Security Centre ("NCSC") '10 Steps to Cyber Security' guidance and will host Council data in accordance with NCSC Cloud Security Principles.

4. The Supplier shall ensure that all staff and contractors with access to Shared Personal Data meet the requirements of the Baseline Personnel Security Standard.

5. The Supplier shall ensure that all staff and contractors with access to Shared Personal Data undertake appropriate Information Governance training.

6. The Supplier shall have appropriate systems and processes in place to adequately identify, assess and manage vulnerabilities. Significant vulnerabilities which could lead to the compromise of Shared Personal Data or other Council information must be notified to the Council Information Security Team via email to [insert applicable email address, e.g.at BHCC information.security@brighton-hove.gov.uk]. Suppliers are expected to notify the Council as soon as is reasonably practicable.

7. The Supplier shall have an appropriate incident management process in place and all security and cyber incidents which affect Shared Personal Data or other Council data and/or the systems on which Shared Personal Data or other Council data resides, or near misses, must be reported without delay to the Council Information Security Team via email to: [insert applicable email address e.g. at BHCC information.security@brighton-hove.gov.uk.]

Schedule 8 - NOT USED

Schedule 9 - NOT USED

Schedule 10: Information to be provided to the Data Subject, where Personal Data have been collected from the Data Subject

Where Personal Data are collected from the Data Subject by the Partner, the Partner shall, at the time such data are obtained (and provided that the Data Subject does not already have such information), provide the Data Subject with the following information:

1. The identity and contact details of themselves as Controller, and where applicable details of a representative;
2. The contact details of the Data Protection Officer, if applicable;
3. The purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing; and
4. The recipients or categories of recipients of the Personal Data, if any;
5. The period for which the Personal Data will be stored or, if that is not possible, the criteria used to determine that period;
6. The existence of the Data Subject's right to request access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to data processing as well as the right to data portability;
7. Where there is no statutory basis for the processing of the Shared Personal Data, and where the processing is based on the Data Subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
8. The right to lodge a complaint with a Regulatory Authority;
9. Whether the provision of the Data Subject's Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data; and
10. Whether the Partner uses the Shared Personal Data for automated decision-making, including profiling.

Schedule 11: Information to be provided to the Data Subject, where Personal Data have not been obtained from the Data Subject

1. Where Personal Data have not been obtained directly from the Data Subject by the Partner, the Partner shall provide the Data Subject with the following information:

    1.1. The identity and contact details of themselves as data controller, and where applicable, the controller's representative;

    1.2. The contact details of the data protection officer, if applicable;

    1.3. The purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing;

    1.4. The categories of Personal Data concerned;

    1.5. The period for which the Personal Data will be stored or, if that is not possible, the criteria used to determine that period;

    1.6. The existence of the Data Subject's right to request access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object top data processing as well as the right to data portability;

    1.7. Where there is no statutory basis for the processing of the Shared Personal Data, and where the processing is based on the Data Subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

    1.8. The right to lodge a complaint with a Regulatory Authority;

    1.9. From which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources; and

    1.10. The existence of automated decision-making, including profiling.

2. This information will be provided by the Partner:

    2.1. Within one month of obtaining the Personal Data; or

    2.2. If the Personal Data is to be used for communication with the Data Subject, at the latest of the time of the first communication to that Data Subject; or

    2.3. If a disclosure to a third party is envisaged, at the latest when the Personal Data are first disclosed.

3. Where a party intends to further process the Personal Data for a purpose other than that for which the Personal Data were obtained, that party shall provide the Data Subject prior to that further processing with information on that purpose.