Schedule 20 (Processing Data)

1. Status of the Controller

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

1.1.1 "Controller" in respect of the other Party who is "Processor";

1.1.2 "Processor" in respect of the other Party who is "Controller";

1.1.3 "Joint Controller" with the other Party;

1.1.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

2. Where one Party is Controller and the other Party its Processor

2.1 Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

2.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

2.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

2.3.1 a systematic description of the envisaged Processing and the purpose of the Processing;

2.3.2 an assessment of the necessity and proportionality of the Processing in relation to the Services;

2.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

2.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

2.4 The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

2.4.1 Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

2.4.2 ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 18.4 of the

Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

a) nature of the data to be protected;

b) harm that might result from a Personal Data Breach;

c) state of technological development; and

d) cost of implementing any measures;

2.4.3 ensure that:

a) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

b) it uses all reasonable endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Processor's duties under this Schedule 20, Clauses 18 (Data protection), 19 (What you must keep confidential) and 20 (When you can share information);

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data;

2.4.4 not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the UK GDPR (or section 73 of DPA 2018); or

b) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time, as well as any additional measures determined by the Controller;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

e) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

2.4.5 where the Personal Data is subject to EU GDPR, not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the EU GDPR; or

b) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the non-transferring Party;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

2.4.6 at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

2.5 Subject to Paragraph 2.6 of this Schedule 20, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

2.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

2.5.2 receives a request to rectify, block or erase any Personal Data;

2.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

2.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

2.5.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

2.5.6 becomes aware of a Personal Data Breach.

2.6 The Processor's obligation to notify under Paragraph 2.5 of this Schedule 20 shall include the provision of further information to the Controller, as details become available.

2.7 Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 2.5 of this Schedule 20 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

2.7.1 the Controller with full details and copies of the complaint, communication or request;

2.7.2 such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

2.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

2.7.4 assistance as requested by the Controller following any Personal Data Breach; and/or

2.7.5 assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.

2.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Schedule 20. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

2.8.1 the Controller determines that the Processing is not occasional;

2.8.2 the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

2.8.3 the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

2.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

2.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

2.11 Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

2.11.1 notify the Controller in writing of the intended Subprocessor and Processing;

2.11.2 obtain the written consent of the Controller;

2.11.3 enter into a written agreement with the Subprocessor which give effect to the terms set out in this Schedule 20 such that they apply to the Subprocessor; and

2.11.4 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

2.12 The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

2.13 The Buyer may, at any time on not less than 30 Working Days' notice, revise this Schedule 20 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

2.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Buyer may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

3. **Where the Parties are Joint Controllers of Personal Data**

3.1 In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Schedule 20 (*Processing Data*).

Independent Controllers of Personal Data

3.2 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

3.3 Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

3.4 Where a Party has provided Personal Data to the other Party in accordance with Paragraph 3.2 of this Schedule 20 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

3.5 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

3.6 The Parties shall only provide Personal Data to each other:

3.6.1 to the extent necessary to perform their respective obligations under the Contract;

3.6.2 in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

3.6.3 where it has recorded it in Annex 1 *(Processing Personal Data).*

3.7 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

3.8 A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

3.9 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

3.9.1 the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

3.9.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

a) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

b) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

3.10 Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

3.10.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

3.10.2 implement any measures necessary to restore the security of any compromised Personal Data;

3.10.3 work with the other Party to make any required notifications to the Information Commissioner's Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

3.10.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

3.11 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

3.12 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

3.13 Notwithstanding the general application of Paragraphs 2.1 to 2.14 of this Schedule 20 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 3.2 to 3.12 of this Schedule 20.

Annex 1 - Processing Personal Data

1. This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

   1.1 The contact details of the Buyer's Data Protection Officer are: [redacted] email: [redacted]

   1.2 The contact details of the Supplier's Data Protection Officer are: [redacted], email: [redacted]

   1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

   1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: ***The provision of the Advocacy 'Safety Net' Service***
Duration of the Processing	Processing will take place from the start of the contract- 1st October 2023 for the duration of the contract. Data will be stored and deleted in accordance with NYAS Records Retention Policy.
Nature and purposes of the Processing	The purpose of the service is to signpost children and young people to locally provided services and to monitor availability. The service will maintain a dynamic picture of local provision, updated via calls to the helpline and based on work with local areas and through its networks. NYAS advocacy will only step in where local advocacy support continues to be denied. There are 3 main elements: 1. A database capturing the availability of local advocacy, which is accurate and kept up to date so to refer children and young people to local support. 2. An advice helpline responding to calls from looked after children and able to respond accordingly, identifying the best route to address concerns. The helpline offers telephone, email, text, and WhatsApp communication options.

	3. Additional advocacy support through web-based information including 'self-advocacy tools and technology. Monitoring and KPI reports provided for contract management requirements (anonymised) Publicly available information on local advocacy providers does not fall under the scope of personal data.
Type of Personal Data	Only the minimum information necessary to provide the Services is to be requested from the Data Subject. *Art. 6 data:* • Full Name, • Contact information: Email, Telephone Number(s) • Address, incl. Post Code • DoB • Issues identified • Lifestyle and social circumstances *Special Category (Art. 9):* • Gender (with option to prefer not to say) • Country of Origin • Ethnicity • Physical or mental health details (incl health or social care records) • Care status • Immigration status .
Categories of Data Subject	*Helpline Staff , NYAS workers,* *Local advocacy providers (publicly available)* *Referrers* *Service Users*- Looked After Children, Care Leavers and young people on the edge of care from 0-25 years old.

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	Data will be retained in accordance with NYAS Data Retention Policy. Electronic information stored on CRM, closed once advocacy ended. Information remains on the system in line with GDPR requirements. No paper files used/stored.
Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract	Data held on [redacted] ([redacted] [redacted] platform) all UK based
Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under this Contract Agreement against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach	*Examples of some of our technical security measures are as follows:* • *Encrypted storage and transfer* • *Pseudonymisation* • *Employee access controls* • *Regular updating of security software and systems* • *Monitoring to detect potential breaches.* • *We adequately dispose of physical files and hardware.* *Examples of some of our Organisational security measures are as follows:* • *Annually reviewed Security and Privacy Policies* • *Employee awareness and training on relevant policies and procedures* • *Undertaking Data Protection Impact Assessments* • *A documented disaster recovery program, including regularly tested backups* • *Limiting employee access to personal data* • *Server rooms are fitted with high security locks which are combined with access control.*

	• *We maintain a risk management program to address information security risks and breaches*

Annex 2 - Joint Controller Agreement

2. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of Paragraph 2 of this Schedule 20 (Where one Party is Controller and the other Party is Processor) and Paragraphs 3.2 - 3.12 of this Schedule 20 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Supplier:

1.2.1 is the exclusive point of contact for Data Subjects and is responsible for using all reasonable endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

1.2.2 shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

1.2.3 is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

1.2.4 is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

1.2.5 shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the Supplier's/ privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of Paragraph 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

3. Undertakings of both Parties

3.1 The Supplier and the Buyer each undertake that they shall:

3.1.1 report to the other Party every 3 months on:

a) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

b) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

c) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

d) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

e) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

3.1.2 notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 3.1.1a) to e);

3.1.3 provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 3.1.1c) to e) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

3.1.4 not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

3.1.5 request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

3.1.6 ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

3.1.7 use all reasonable endeavours to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

a) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

b) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

c) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

3.1.8 ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

a) nature of the data to be protected;

b) harm that might result from a Personal Data Breach;

c) state of technological development; and

d) cost of implementing any measures;

3.1.9 ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

3.1.10 ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach;

3.1.11 where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the UK GDPR or DPA 2018 Section 73; or

b) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which could include the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time, as well as any additional measures;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

3.1.12 where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of non-transferring Party has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the EU GDPR; or

b) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU as well as any additional measures;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the transferring Party complies with its obligations under the EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

3.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

4. Data Protection Breach

4.1 Without prejudice to Paragraph 4.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are

likely to give rise to a Personal Data Breach, providing the Buyer and its advisors with:

4.1.1 sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

4.1.2 all reasonable assistance, including:

a) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

b) co-operation with the other Party including using such reasonable endeavours as are directed by the Buyer to assist in the investigation, mitigation and remediation of a Personal Data Breach;

c) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

d) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Paragraph 4.2.

4.2 Each Party shall use all reasonable endeavours to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

4.2.1 the nature of the Personal Data Breach;

4.2.2 the nature of Personal Data affected;

4.2.3 the categories and number of Data Subjects concerned;

4.2.4 the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

4.2.5 measures taken or proposed to be taken to address the Personal Data Breach; and

4.2.6 describe the likely consequences of the Personal Data Breach.

5. **Audit**

5.1 The Supplier shall permit:

5.1.1 the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

5.1.2 the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

5.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 5.1 in lieu of conducting such an audit, assessment or inspection.

6. **Impact Assessments**

The Parties shall:

6.1 provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

6.2 maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

7. **ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

8. **Liabilities for Data Protection Breach**

8.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

8.1.1 if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the

payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

8.1.2 if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

8.1.3 if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 39 of the Core Terms (Resolving disputes).

8.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

8.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

8.3.1 if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

8.3.2 if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

8.3.3 if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

8.4 Nothing in either Paragraph 8.2 or Paragraph 8.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

9. **Termination**

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 14 of the Core Terms (Ending the contract).

10. **Sub-Processing**

In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

10.1 carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

10.2 ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

11. **Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.