DATED 06/12/2021

(1) Age UK Nottingham & Nottinghamshire

(2) Studio Chocolate

DATA PROCESSING & CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made the 6th Day of December 2021

BETWEEN:

(1) Age UK Nottingham & Nottinghamshire (Age UK Notts), a company registered in the United Kingdom under number ***3455485***, whose registered office is at Bradbury House, 12 Shakespeare Street, Nottingham, NG1 4FQ ("Data Controller").

(2) Studio Chocolates, whose registered office is at First Floor, 8 Thurland Street, Nottingham, NG1 3DR ("Data Processor")

WHEREAS:

(1) Under a written agreement between the Data Controller and the Data Processor dated 6th December 2021 ("the Service Agreement") the Data Processor provides to the Data Controller the Services described in Schedule 1 utilising nominated Users and employees.

(2) The provision of the Services by the Data Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Data Controller.

(3) Under the Data Protection Act 2018, the Data Controller is required to put in place an agreement in writing between the Data Controller and any organisation which processes personal data on its behalf governing the processing of that data.

(4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the Data Protection Act in relation to all processing of the Personal Data by the Data Processor for the Data Controller.

(5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller by the Data Processor and to all Personal Data held by the Data Processor in relation to all such processing.

IT IS AGREED as follows:

1. **Definitions and Interpretation**

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Data Controller", "Data Processor", "processing", and "data subject"	shall have the meanings given to the terms "controller", "processor", "processing", and "data subject";
"ICO"	means the UK's supervisory authority, the Information Commissioner's Office;
"Personal Data"	means all such "personal data", as defined in the Data Protection Act 2018, as is, or is to be, processed by the Data Processor on behalf of the Data Controller, as described in Schedule 2;

"Services"	means those services described in Schedule 1 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purpose**[**s**]** described in Schedule 1;
"Sub-Processor"	means a sub-processor appointed by the Data Processor to process the Personal Data; and

1.2 Unless the context otherwise requires, each reference in this Agreement to:

1.2.1 "writing", and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;

1.2.2 a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

1.2.3 "this Agreement" is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

1.2.4 a Schedule is a schedule to this Agreement; and

1.2.5 a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.

1.2.6 a "Party" or the "Parties" refer to the parties to this Agreement.

1.3 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4 Words imparting the singular number shall include the plural and vice versa.

1.5 References to any gender shall include all other genders.

1.6 References to persons shall include corporations.

2. Scope and Application of this Agreement

2.1 The provisions of this Agreement shall apply to the processing of the Personal & Commercial Data described in Schedule 2, carried out for the Data Controller by the nominated Users and employees of the Data Processor, and to all Personal Data held by the Data Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.

2.2 The provisions of this Agreement supersede any other arrangement, understanding, or agreement made between the Parties at any time relating to the Personal Data.

2.3 This Agreement shall continue in full force and effect for so long as the nominated Users and employees of the Data Processor is processing Personal Data on behalf of the Data Controller, and thereafter as provided in Clause 9.

3. Provision of the Services and Processing Personal Data

The nominated Users and employees of the Data Processor are only to carry out the Services, and only to process the Personal Data received from the Data Controller:

3.1 for the purposes of those Services and not for any other purpose;

3.2 to the extent and in such a manner as is necessary for those purposes; and

3.3 strictly in accordance with the express written authorisation and instructions of the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor).

4. **Data Protection Compliance**

4.1 All instructions given by the Data Controller to the nominated Users and employees of the Data Processor shall at all times be in compliance with the Data Protection Act 2018 and other applicable laws. The Data Processor shall act only on instructions from the Data Controller unless the Data Processor is required by law to do otherwise.

4.2 The nominated Users and employees of the Data Processor shall promptly comply with any request from the Data Controller requiring them to amend, transfer, delete, or otherwise dispose of the Personal Data.

4.3 The nominated Users and employees of the Data Processor shall transfer all Personal Data to the Data Controller on the Data Controller's request in the formats, at the times, and in compliance with the Data Controller's instructions.

4.4 Both Parties shall comply at all times with the DATA PROTECTION ACT 2018 and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such way as to cause either Party to breach any of its applicable obligations under the DATA PROTECTION ACT 2018.

4.5 The Data Controller hereby warrants, represents, and undertakes that the Personal Data shall comply with the DATA PROTECTION ACT 2018 in all respects including, but not limited to, its collection, holding, and processing.

4.6 The nominated Users and employees of the Data Processor agree to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force (including, but not limited to, the DATA PROTECTION ACT 2018) and any best practice guidance issued by the ICO.

4.7 The nominated Users and employees of the Data Processor shall provide all reasonable assistance (at the Data Controller's cost) to the Data Controller in complying with its obligations under the DATA PROTECTION ACT 2018 with respect to the security of processing, the notification of personal data breaches, the conduct of data protection impact assessments, and in dealings with the ICO.

4.8 When processing the Personal Data on behalf of the Data Controller, the nominated Users and employees of the Data Processor shall:

4.8.1 not process the Personal Data outside the United Kingdom without the prior written consent of the Data Controller and, where the Data Controller consents to such a transfer to a country that is outside of the EEA, to comply with the obligations of Data Processors under the provisions applicable to transfers of Personal Data to third countries set out in Chapter 5 of the DATA PROTECTION ACT 2018 by providing an adequate level of protection to any Personal Data that is transferred;

4.8.2 not transfer any of the Personal Data to any third party without the written consent of the Data Controller and, in the event of such

consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 10;

4.8.3 process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Data Controller or as may be required by law.

4.8.4 implement appropriate technical and organisational measures, as described in Schedule 3, and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure.

4.8.5 if so requested by the Data Controller (and within the timescales required by the Data Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

4.8.6 keep detailed records of all processing activities carried out on the Personal Data in accordance with the requirements of Article 30(2) of the DATA PROTECTION ACT 2018;

4.8.7 make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the nominated Users and employees of the Data Processor's compliance with the DATA PROTECTION ACT 2018;

4.8.8 with notice, submit to audits and inspections and provide the Data Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties' compliance with the requirements of the DATA PROTECTION ACT 2018. The requirement to give notice will not apply if the Data Controller believes that the nominated Users and employees of the Data Processor are in breach of any of obligations under this Agreement or under the law; and

4.8.9 inform the Data Controller immediately if it is asked to do anything that infringes the DATA PROTECTION ACT 2018 or any other applicable data protection legislation.

5. **Data Subject Access, Complaints, and Breaches**

5.1 The nominated Users and employees of the Data Processor shall, at the Data Controller's cost, assist the Data Controller in complying with its obligations under the DATA PROTECTION ACT 2018. In particular, the following shall apply to data subject access requests, complaints, and data breaches.

5.2 The nominated Users or employees of the Data Processor shall notify the Data Controller without undue delay if it receives:

5.2.1 a subject access request from a data subject; or

5.2.2 any other complaint or request relating to the processing of the Personal Data.

5.3 The nominated Users and employees of the Data Processor shall, at the Data Controller's cost, cooperate fully with the Data Controller and assist as required in relation to any subject access request, complaint, or other request, including by:

5.3.1 providing the Data Controller with full details of the complaint or request;

5.3.2 providing the necessary information and assistance in order to comply with a subject access request;

5.3.3 providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller); and

5.3.4 providing the Data Controller with any other information requested by the Data Controller.

5.4 The nominated Users and employees of the Data Processor shall notify the Data Controller immediately if it becomes aware of any form of Personal Data breach, including any unauthorised or unlawful processing, loss of, damage to, or destruction of any of the Personal Data.

6. Appointment of a Data Protection Officer

6.1 The Data Controller has appointed a Data Protection Officer in accordance with the DATA PROTECTION ACT 2018, whose details are as follows: Michelle Elliott, Assistant Chief Executive (Resources)

7. Liability and Indemnity

7.1 The Data Controller shall be liable for, and shall indemnify (and keep indemnified) the Data Processor in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the nominated Users and employees of the Data Processor arising directly or in connection with:

7.1.1 any non-compliance by the Data Controller with the DATA PROTECTION ACT 2018 or other applicable legislation;

7.1.2 any Personal Data processing carried out by the nominated Users or employees of the Data Processor in accordance with instructions given by the Data Controller that infringe the DATA PROTECTION ACT 2018 or other applicable legislation; or

7.1.3 any breach by the Data Controller of its obligations under this Agreement,

except to the extent that the nominated Users and employees of the Data Processor are liable under sub-Clause 7.2.

7.2 The Data Processor shall be liable for, and shall indemnify (and keep indemnified) the Data Controller in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Controller arising directly or in connection with the nominated Users and employees of the Data Processor's Personal Data processing activities that are subject to this Agreement:

7.2.1 only to the extent that the same results from the nominated Users and employees of the Data Processor's breach of this Agreement; and

7.2.2 not to the extent that the same is or are contributed to by any breach of this Agreement by the Data Controller.

7.3 The Data Controller shall not be entitled to claim back from the Data Processor any sums paid in compensation by the Data Controller in respect of

any damage to the extent that the Data Controller is liable to indemnify the Data Processor under sub-Clause 7.1.

7.4 Nothing in this Agreement (and in particular, this Clause 7) shall relieve either Party of, or otherwise affect, the liability of either Party to any data subject, or for any other breach of that Party's direct obligations under the DATA PROTECTION ACT 2018. Furthermore, the Data Processor hereby acknowledges that it shall remain subject to the authority of the ICO and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data processor under the DATA PROTECTION ACT 2018 may render it subject to the fines, penalties, and compensation requirements set out in the DATA PROTECTION ACT 2018.

8. Intellectual Property Rights

All copyright, database rights, and other intellectual property rights subsisting in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Data Controller or the nominated Users or employees of the Data Processor) shall belong to the Data Controller or to any other applicable third party from whom the Data Controller has obtained the Personal Data under licence (including, but not limited to, data subjects, where applicable). The Data Processor is licensed to use such Personal Data under such rights only for the purposes of the Services, and in accordance with this Agreement.

9. Confidentiality

9.1 The nominated Users and employees of the Data Processor shall maintain the Personal & Commercial Data in confidence, and in particular, unless the Data Controller has given written consent for the nominated Users and employees of the Data Processor to do so, the nominated Users and employees of the Data Processor shall not disclose any Personal or Commercial Data supplied to the nominated Users and employees of the Data Processor by, for, or on behalf of, the Data Controller to any third party. The nominated Users and employees of the Data Processor shall not process or make any use of any Personal & Commercial Data supplied to it by the Data Controller otherwise than in connection with the provision of the Services to the Data Controller.

9.2 The Data Processor shall ensure that all personnel who are to access and/or process any of the Personal& Commercial Data are contractually obliged to keep the Personal & Commercial Data confidential.

9.3 The obligations set out in in this Clause 9 shall continue after the cessation of the provision of Services by the Data Processor to the Data Controller.

9.4 Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.

10. Appointment of Sub-Processors

10.1 The Data Processor shall not sub-contract any of its obligations or rights under this Agreement without the prior written consent of the Data Controller (such consent not to be unreasonably withheld).

11. **Deletion and/or Disposal of Personal Data**

11.1 The nominated Users and employees of the Data Processor shall, at the request of the Data Controller, delete (or otherwise dispose of) the Personal Data or return it to the Data Controller in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of the following:

11.1.1 the end of the provision of the Services; or

11.1.2 the processing of that Personal Data by the nominated Users or employees of the Data Processor is no longer required for the performance of the Data Processor's obligations under this Agreement**.**

11.2 Following the deletion, disposal, or return of the Personal Data under sub-Clause 11.1, the Data Processor shall delete (or otherwise dispose of) all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case the Data Processor shall inform the Data Controller of such requirement(s) in writing.

12. **Law and Jurisdiction**

12.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

12.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

SIGNED for and on behalf of the Data Controller by:

Name : Michelle Elliott

_____

Authorised Signature

Date: _____

SIGNED for and on behalf of the Data Processor by:

Name :

_____

Authorised Signature

Date: _____

SCHEDULE 1

Services

Studio Chocolates are to provide chocolates to the volunteers of Age UK Nottingham & Nottinghamshire. These services are in the form of the following:

- Posting chocolates to the home address of all Volunteers of Age UK Nottingham & Nottinghamshire.

SCHEDULE 2

Personal Data

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing
Names & home addresses,	Volunteers	Receiving, handling and storing	To post chocolates to volunteer home addresses	Until the final box of chocolates has been posted

SCHEDULE 3

Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 4:

1. The Data Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Data Controller, it maintains security measures to a standard appropriate to:
   1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and
   1.2 the nature of the Personal Data.

2. In particular, the Data Processor shall:
   2.1 have in place, and comply with, a security policy which:
      2.1.1 defines security needs based on a risk assessment;
      2.1.2 allocates responsibility for implementing the policy to a specific individual **[**(such as the Data Processor's Data Protection Officer)**]** or personnel;
      2.1.3 is provided to the Data Controller on or before the commencement of this Agreement;
      2.1.4 is disseminated to all relevant staff; and
      2.1.5 provides a mechanism for feedback and review.
   2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;
   2.3 prevent unauthorised access to the Personal Data;
   2.4 protect the Personal Data using pseudonymisation, where it is practical to do

so;

2.5 ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

2.6 have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using <<insert type of encryption>> encryption);

2.7 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure (<<describe requirements, e.g. upper and lower-case letters, special characters etc.>>), and that passwords are not shared under any circumstances;

2.8 **[**not allow the storage of the Personal Data on any mobile devices such as laptops or tablets unless such devices are kept on its premises at all times;**]**

2.9 take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;

2.10 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

2.10.1 the ability to identify which individuals have worked with specific Personal Data;

2.10.2 having a proper procedure in place for investigating and remedying breaches of the DATA PROTECTION ACT 2018; and

2.10.3 notifying the Data Controller as soon as any such security breach occurs.

2.11 have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;

2.12 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; and

2.13 adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the Services provided to the Data Controller.