ENGAGE SOLUTIONS GROUP

DP POLICY

1. DEFINITIONS

In this Policy, the following terms shall have the following meanings:

"**controller**", "**data controller**", "**data processor**", "**processor**", "**data subject**", "**personal data**", "**personal data breach**", "**processing**" (and "**process**"), "**sensitive personal data**" and "**special categories of personal data**" shall have the meanings given in Applicable Data Protection Law;

"**Applicable Data Protection Law**" shall mean data protection law, including legislation and regulations, applicable in the UK from time to time including the Data Protection Act 2018 and the UK General Data Protection Regulation ("GDPR")

"**Data Protection Legislation**" shall mean**:**

(a) the Data Protection Act 2018 (the "**Data Protection Act**");

(b) the EU General Data Protection Regulation (Regulation 2016/679) (the "**GDPR**");

(c) any legislation which implements or supplements the GDPR in the UK.

References in this Policy to personal data shall relate only to personal data of which the Client is the Controller/Data Controller (whether jointly or individually) and in relation to which the Supplier is providing Services and/or otherwise processing under this Agreement ("**Personal Data**")

2. RELATIONSHIP OF THE PARTIES / OBLIGATIONS OF THE SUPPLIER

2.1 The Client appoints the Supplier as a processor to process the Personal Data for the purpose of making the Solution available and performing the Services in the manner set out in the agreement (the "**Purpose**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law in respect of Personal Data and in so doing:.

2.1.1 the Supplier shall process the Personal Data only to the extent, and in such a manner, as is necessary for the Purpose and in accordance with the Client's documented instructions from time to time (which may be by email) and shall not process the Personal Data for any other purpose (save where otherwise required by law, in which case the Supplier must inform the Client of such legal requirement before processing, unless such law prohibits such information being provided to the Client on important grounds of public interest).

2.1.2 from 25 May 2018, the Supplier will :

(a) keep a record of any processing of Personal Data it carries out on behalf of the Client to the extent required by Applicable Data Protection Law; and

(b) where, in the Supplier's opinion, any instruction of the Client infringes any Applicable Data Protection Law, immediately inform the Client.

3. INTERNATIONAL TRANSFERS

The Supplier shall not transfer the Personal Data outside the European Economic Area without the prior written consent of the Client. If the Client, in its discretion, consents to this transfer (having

first been given full details of the proposal), the Supplier shall not transfer the Personal Data outside of the European Economic Area ("**EEA**") unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. If the Client does not provide its consent to the transfer, either party shall be entitled to terminate this Agreement by serving not less than 4 months' notice in writing to the other party (without prejudice to any fees payable for the Services prior to termination).

4. CONFIDENTIALITY OF PROCESSING/ SUPPLIER'S AUTHORISED PERSONNEL.

4.1 The Supplier shall ensure that any person it authorises to process the Personal Data (an "**Authorised Person**" and "**Authorised Personnel**") shall protect the Personal Data in accordance with the Supplier's confidentiality obligations under the agreement.

4.1.1 The Supplier shall ensure that access to the Personal Data is limited to:

(a) those Authorised Personnel who need access to the Personal Data to meet the Supplier's obligations under this Agreement; and

(b) in the case of any access by any Authorised Person, such part or parts of the Personal Data as is strictly necessary for performance of that Authorised Person's duties.

4.1.2 The Supplier shall ensure that all Authorised Personnel:

(a) are informed of the confidential nature of the Personal Data and are obliged to treat such Personal Data accordingly;

(b) have undertaken training in the laws relating to handling personal data; and

(c) are aware both of the Supplier's duties and their personal duties and obligations under such laws and this Agreement.

4.1.3 The Supplier shall take reasonable steps to ensure the reliability of any of the Supplier's Authorised Personnel who have access to the Personal Data.

5. SECURITY

5.1 The Supplier warrants that it will implement appropriate technical and organisational measures:

(i) against the unauthorised or unlawful access or alteration to and/or processing of Personal Data; and

(ii) against the accidental or unauthorised loss or destruction of, or damage to Personal Data;

to ensure a level of security appropriate to the risk, 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. The Supplier shall provide a description of these measures to the Client on request.

6. SUBCONTRACTING

6.1 The Client authorises the Supplier's appointment of Amazon Web Services as a sub-processor to provide hosting services in respect of the Personal Data for the duration of the Agreement.

6.2 The Supplier shall:

(a) not authorise any other third party (”**Sub-Processor**”) to process the Personal Data without the prior written consent of the Client;

(b) when seeking the Client's consent to the appointment of a Sub-Processor, provide details of the proposed Sub-Processor to the Client, including its identity and the processing activities which it will perform for the Supplier, and any further information about the appointment of the proposed Sub-Processor which is reasonably requested by the Client ; and

(c) impose data protection terms on any Sub-Processor it appoints that are substantially the same as those set out in this Policy and in such manner that it meets the requirements of Applicable Data Protection Law.

6.3 Where the Client objects to the Supplier's proposed appointment or replacement of a Sub-Processor prior to its appointment or replacement on the grounds of Applicable Data Protection Law, it shall notify the Supplier within10 Business Days of the Supplier's notification of the proposed change, and if the parties are subsequently unable to reach agreement on the appointment of the Sub-Processor, the Supplier shall either not appoint the Sub-Processor or shall give the Client [4] months’ written notice that it intends to appoint the Sub-Processor, and the Client or the Supplier shall be entitled to terminate this Agreement on written notice to the other party, such termination to take effect on expiry of the [4] month notice period (without prejudice to any fees payable for the Services prior to termination).

7. COOPERATION AND DATA SUBJECTS' RIGHTS

7.1 Taking into account the nature of the processing of Personal Data performed by the Supplier, the [Supplier shall assist the Client by taking appropriate technical and organisational measures (insofar as this is possible) to enable the Client to respond to:

(a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) in respect of Personal Data; and

(b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Personal Data,

subject to the Client paying the reasonable charges and expenses of the Supplier, such charges and expenses to be agreed in advance in writing.

.

7.2 The Supplier shall:

(a) notify the Client in writing as soon as reasonably possible and in any event within 3 Business Days if it receives a request from a Data Subject for access to that person’s Personal Data;

(b) not disclose the Personal Data to any Data Subject or to a third party other than at the written request of the Client or as provided for in this Agreement unless required to do so at law or lawfully by a regulatory body.

In the event that any request, correspondence, enquiry or complaint is made directly to the Supplier in connection with any Personal Data processed by the Supplier under this agreement, the Supplier shall promptly inform the Client providing full details of the same (save where it is prohibited from so doing by applicable law or regulatory requirements).

8. DATA PROTECTION IMPACT ASSESSMENT

If Client believes or becomes aware that its processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform the Supplier and the Supplier shall provide reasonable cooperation with and assistance to the Client in connection with any data protection impact assessment, that may be required by the Client under Applicable Data Protection Law, or otherwise in providing reasonable assistance to the Client in complying with its obligations under Articles 35 and 36 of the GDPR subject to the Client paying the reasonable charges and expenses of the Supplier, such charges and expenses to be agreed in advance in writing.

9. SECURITY INCIDENTS

9.1 If it becomes aware of a personal data breach in respect of the Personal Data, the Supplier shall inform the Client promptly and without undue delay and shall provide reasonable information and cooperation to the Client so that the Client can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. In so doing, the Supplier shall inform the Client of:

(a) the nature of the personal data breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) to the extent that the Supplier has knowledge of this, the likely consequences of the personal data breach;

(c) any measures taken or proposed to be taken to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects; and

(d) the name and contact details of the Supplier's contact who can supply further information.

Where the Supplier is unable to provide all the requisite information at the same time, it may be provided in phases without undue further delay.

9.2 The Supplier shall further take reasonably necessary measures and actions to remedy or mitigate the effects of the personal data breach, implement its disaster recovery and business continuity procedures which shall including restoring data to the last available recovery point of the affected Personal Data (save where to do so would exacerbate the personal data breach) and shall keep the Client informed of all material developments in connection with the personal data breach.

10. DELETION OR RETURN OF DATA

Upon termination or expiry of the agreement (or the provision of any Services, whichever is the later), the Supplier shall (at the Client's election) destroy or return to the Client all Personal Data in its possession or control. This requirement shall not apply to the extent that the Supplier is required by applicable law to retain some or all of the Personal Data. The Supplier shall securely isolate and protect such Personal Data from any further processing except to the extent required by law. The Supplier shall inform the Client of any Personal Data which it is required to retain, including details as to the required retention period.

11. AUDIT

11.1 The Supplier will make available to the Client all information necessary to demonstrate compliance with its obligations set out in this Policy and Applicable Data Protection Law in respect of the Supplier's processing of the Personal Data, and will permit and contribute to audits and inspections by the Client as follows:

(a) engage in dialogue with the Client's personnel/auditors;

(b) provide documented responses to any reasonable requests made by the Client's personnel/auditors in this respect;

(c) share any third party audit reports in this respect which are in the Supplier's possession at the time of the request and which are relevant to this DP Policy;

(d) provide for the Client's inspection, copies of such records.

all of which shall be subject to the confidentiality provisions of the Agreement.

11.3 Where the Client exercises its audit and inspection rights more than once in any 12 month period, any costs or expenses incurred by the Supplier in complying with the Client's request shall be paid by the Client