Schedule 11 - Data Protection

1 General

1.1 Details of the Processing of Personal Data carried out by the Supplier under or in connection with this Agreement are set out in Annex B to this Schedule 11. Annex B includes details of whether the Supplier is Processing Personal Data as a Data Controller (in which case the obligations set out in Clause 23.2 (Protection of Personal Data) apply to such Processing) or as a Data Processor (in which case the obligations set out in this Schedule 11 (Data Protection) apply to such Processing).

1.2 The Parties agree and acknowledge that where the Supplier is Processing Personal Data on behalf of the Authority:

1.2.1 the Authority alone shall determine the purposes for which, and the manner in which, Personal Data is, or is to be, Processed in the provision of the Services or otherwise in connection with this Agreement; and

1.2.2 the parties shall comply with their respective obligations set out in this Schedule 11 (Data Protection).

1.3 The Supplier warrants that it has in place, and undertakes that it shall maintain, appropriate technical and organisational measures to ensure that the Processing of Personal Data by the Supplier in connection with this Agreement meets the requirements of the Data Protection Legislation, including ensuring the protection of the rights of Data Subjects in accordance with the Data Protection Legislation. Such technical and organisational measures shall include (without limitation) the measures set out in Annex A.

2 Restrictions

2.1 The Supplier shall not disclose Personal Data to any Data Subject or to a third party other than:

2.1.1 at the request of the Authority;

2.1.2 as provided for in this Agreement; or

2.1.3 to the extent required under a court order by a court of competent jurisdiction (provided that the Supplier shall give notice to the Authority of any disclosure of Personal Data that it, or any of the Supplier's Sub-contractors, is required to make under such a court order as soon as practicable when it is made aware of such a requirement).

2.2 The Supplier shall:

2.2.1 Process the Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments (including the Data Protection Legislation);

2.2.2 Process the Personal Data only to the extent, and in such a manner, as is necessary for the Permitted Purposes and in accordance with the Authority's written instructions from time to time and shall not Process the Personal Data for any other purposes; and

2.2.3 notify the Authority in writing immediately if, in its reasonable opinion, it considers that any instruction infringes the Data Protection Legislation.

2.3 For the avoidance of doubt, except as expressly set out in this Agreement, the Supplier shall not be required to ensure that its provision of the Services or its other obligations under this Agreement comply with the provisions of the GDPR until 25 May 2018, although it may expressly elect or agree in writing to become compliant before that date.

3 Data Collection

3.1 The Supplier shall only collect any Personal Data on behalf of the Authority in the form agreed with the Authority which will contain a data protection notice informing the Data Subject of the identity of the Data Controller, the identity of any data protection representative it may have appointed, the purpose or purposes for which the Data Subject's Personal Data will be processed and any other information which is necessary to comply with the Data Protection Legislation. The Supplier shall not modify or alter the form in any way without the prior written consent of the Authority.

4 Data Security and Breach Notification

4.1 The Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the Processing of Personal Data pursuant to this Agreement, including (without limitation) the risks presented by a Personal Data Breach. Such measures shall include (without limitation):

4.1.1 the pseudonymisation and encryption of Personal Data where appropriate in accordance with good industry practice;

4.1.2 measures to ensure the on-going confidentiality, integrity, availability and resilience of the systems used for Processing and the provision of the Services;

4.1.3 measures to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

4.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing; and

4.1.5 such other security measures as are set out in Annex C and the Schedule 2.4 (Security Management).

4.2 The Supplier shall notify the Authority in writing within 24 hours if it becomes aware of:

4.2.1 any Personal Data Breach (whether caused by the Supplier or otherwise); and/or

4.2.2 any advance in technology and methods of working or potential security threats which mean that the Parties should revise the security measures taken by the Supplier to comply with its obligations under this Paragraph 4 (including as set out in Annex C) or as set out in Schedule 2.4 (Security Management).

4.3 Where the Supplier notifies the Authority of advances in technology or methods of working or potential security threats that mean the Parties should revise the security measures set out in Annex C, the Parties shall agree appropriate changes to Annex C in accordance with the Change Control Procedure.

4.4 Where a Personal Data Breach occurs the Supplier shall provide such information and assistance and take such steps as the Authority may reasonably require to enable the Authority:

4.4.1 to mitigate the impact of the Personal Data Breach;

4.4.2 to ensure that Personal Data Breaches of the same nature do not occur again;

4.4.3 to notify the competent regulatory body of the Personal Data Breach; and/or

4.4.4 to notify Data Subjects of the Personal Data Breach.

5 Co-Operation and Assistance

5.1 The Supplier shall provide the Authority with all reasonable co-operation and assistance in relation to the Processing of Personal Data to ensure that the Authority is

able to comply with all of its obligations under the Data Protection Legislation, including (without limitation):

5.1.1 implementing appropriate technical and organisational measures to assist the Authority to fulfil its obligations to respond to requests from Data Subjects made under the Data Protection Legislation (including Data Subject Access Requests);

5.1.2 upon request putting in place measures to restrict the Processing of Personal Data;

5.1.3 upon request providing a copy of Personal Data relating to specific Data Subjects in a structured, commonly used and machine readable format;

5.1.4 upon request providing a copy of the record of any Processing of Personal Data it carries out on behalf of the Authority including (without limitation) the records specified in Article 30(2) of the GDPR;

5.1.5 upon request providing information about the Supplier's Processing of Authority Data;

5.1.6 assisting the Authority with the preparation of data protection impact assessments and preparing data protection impact assessments on behalf of the Authority on request;

5.1.7 upon request providing a written description of the technical and organisational methods referred to in Paragraph 4 (Data security and breach notification). Within 30 days of such a request, the Supplier shall provide written particulars of all such measures to a reasonable level of details such that the Authority can determine whether, in connection with the Personal Data, the Data Protection Legislation is being complied with;

5.1.8 promptly complying with any request from the Authority requiring the Supplier to amend, transfer or delete the Personal Data and/or Authority Data; and

5.1.9 subject to the Supplier being required to maintain such copies by law, upon expiry or termination of the Services (for any reason whatsoever), the Supplier shall at the request of the Authority promptly return to the Authority or destroy all Personal Data and/or Authority Data securely (regardless of form, and whether computerised or physical) and shall certify the deletion or destruction (as applicable) to the Authority in writing.

6 Individuals' Rights

6.1 The Supplier shall notify the Authority promptly and in any event within 2 Working Days if it receives a request from a Data Subject wishing to exercise any of the Data Subject's rights under the Data Protection Legislation.

6.2 The Supplier shall notify the Authority immediately and in any event within 2 Working Days and provide all reasonable co-operation and assistance if:

6.2.1 it receives any complaint, notice or communication not covered under Paragraph 6.1 which relates directly or indirectly to the Processing of the Personal Data or to either Party's compliance with the Data Protection Legislation; or

6.2.2 the Supplier is subject to any regulatory investigation by the Information Commissioner or any other data protection supervisory authority.

6.3 The Supplier shall not without the prior written consent of the Authority or as strictly necessary to perform the Services, carry out Processing by automatic means of any Personal Data and/or Authority Data for the purposes of evaluating matters about a Data Subject that constitutes the sole basis for any decision that significantly affects such Data Subjects.

7 Overseas Data Transfers

7.1 The Supplier shall not transfer the Personal Data to a country outside the United Kingdom without the prior written consent of the Authority and subject to compliance with such reasonable conditions as the Authority may specify.

8 Supplier Personnel

8.1 The Supplier shall ensure that access to the Personal Data and/or Authority Data is limited to:

8.1.1 the Supplier Personnel who need access to the Personal Data and/or Authority Data to enable the provision of the Services (provided that such access is subject to written terms substantially the same as, and no less stringent than, the terms contained in Clause 23.2 of this Agreement and this Schedule); and

8.1.2 in the case of any access by any Supplier Personnel, such part or parts of the Personal Data and/or Authority Data as is strictly necessary for performance of that Supplier Personnel's duties.

8.2 The Supplier shall ensure that all Supplier Personnel involved in the Processing of the Personal Data and/or Authority Data:

8.2.1 are informed of the confidential nature of the Personal Data and/or Authority Data;

8.2.2 are subject to legally binding obligations of confidentiality in relation to the Personal Data;

8.2.3 have undertaken reasonably adequate training in the laws relating to care and handling Personal Data and/or Authority Data; and

8.2.4 are aware both of the Supplier's duties and their personal duties and obligations under such laws and this Contract.

8.3 The Supplier shall take reasonable steps to ensure the reliability of any of the Supplier Personnel who have access to the Personal Data and/or Authority Data.

9 Sub-contractors

9.1 The Supplier may only authorise a Sub-contractor to Process the Personal Data:

9.1.1 subject to the Authority's prior written consent where the Supplier has supplied the Authority with full details of such Sub-contractor;

9.1.2 provided that such Sub-contractor's contract is on terms which impose the same or equivalent data protection obligations on the Sub-contractor as those imposed on the Supplier as set out in Clause 23.2 of this Agreement and this Schedule, including, but not limited to, the requirement to implement appropriate technical and organisational measures to ensure that the Processing will meet the requirements set out in the Data Protection Legislation;

9.1.3 provided that such Sub-contractor shall where requested enter into a confidentiality undertaking with the Authority (in a form specified by the Authority);

9.1.4 provided that such Supplier Subcontractor's contract terminates automatically on termination of this Agreement for any reason.

9.2 In accordance with Paragraph 9.1.1, the Authority expressly consents to the Processing of Personal Data by the Supplier's Sub-contractors listed in Schedule 4.3 (Notified Key Sub-contractors).

9.3 For the avoidance of doubt, where a Sub-contractor fails to comply with its data protection obligations, the Supplier shall remain liable to the Authority for the performance of the Sub-contractor's obligations.

10 Records, Information and Audit Rights

10.1 The Supplier shall keep a record of any Processing of Personal Data it carries out on behalf of the Authority including (without limitation) from and including 25 May 2018 the records specified in Article 30(2) of the GDPR.

10.2 The Authority is entitled, on giving reasonable notice of no fewer than 5 Working Days to the Supplier, and the Supplier shall permit the Authority, to inspect or appoint representatives to inspect all facilities, equipment, documents and electronic data relating to the Processing of Personal Data by the Supplier for the purpose of verifying the Supplier's compliance with the Data protection provisions of this Agreement and this Schedule.

10.3 The requirement under Paragraph 10.2 to give notice will not apply if the Authority reasonably believes that the Supplier is in material breach of any of its obligations under this Agreement or the Data Protection Legislation.

Annex A

Technical and Organisational Measures to ensure compliance with Data Protection Legislation

See attached details of G4S policies, procedures and other measures inserted.

G4S_ Data Protection Policy

[REDACTED]

G4S_ Subject Access Requests--Guidance Notes-

[REDACTED]

AIC Operator Process

[REDACTED]

Annex B

Details of Supplier Processing Activities

[REDACTED]

Annex C

Security Measures

See attached G4S Security Policies.

Group Information Security Policy Standard

[REDACTED]

Group Information Security Controls Standard

[REDACTED]

G4S Group Acceptable Use Policy

[REDACTED]

G4S Google Endpoint Policy and Standard

[REDACTED]

G4S Google Data Processing Policy

[REDACTED]