Dated the 23rd day of May 2018

CARE QUALITY COMMISSION

And

CHOICE SUPPORT

Deed of Variation

For

CONTRACT
relating to the supply of
Experts by Experience Services for Year 3
and Contract Extension Period
LOT 2 – CENTRAL REGION

THIS Deed is made the 23rd day of May 2018

Care Quality Commission of 151 Buckingham Palace Road, London SW1W 9SZ **("the Authority")** of the one part; and

Choice Support a company (Company number 2189556) whose registered office is at 100 Westminster Bridge Road, London, SE1 7XA and Choice Support a charity (charity registered number 298149) whose registered address is 100 Westminster Bridge Road, London SE1 7XA **("the Contractor").**

(collectively hereafter referred to as **"the Parties"** and individually **"the Party")**

RECITALS

1. The Parties entered into a contract ("the Contract") dated 24th March 2016 for an Initial Contract Period of 18 months from 1st February 2016 to 31st July 2017 for the provision of Experts by Experience Services **("the Services")**.

2. On 9th October 2017 the parties entered into a Deed of Variation ("First Variation") and agreed the following;

    a. variation of the Initial Contract Term to extend it by ten months from 1st August 2017 until 31st May 2018, (for the avoidance of doubt (the Parties acknowledged that the period of 1st February 2018 to 31st May 2018 would constitute Year 3 of the Contract and would be subject to terms contained in the original Contract in respect of volumes and fixed costs);
    b. the Key Performance Indicators (KPIs) numbered 1 and 3, listed in Schedule 4 of the Contract and contained within Annex 1 of the Deed of Variation dated 9th October 2017 were deleted and replaced with the KPIs contained with Annex 1A of the said Deed of Variation;
    c. the Authority's Social Value Requirements and the Contractor's response to the Authority's Social Value Requirements contained within Annex 2 of the Deed of Variation were inserted as Annex 8, Social Value Requirements to Schedule 1 (Specification) of the Contract;
    d. a new Schedule 3A (Pricing for Social Value Requirements) which contained the Social Value Costs set out in Annex 3 of the said Deed of Variation; and

e. a new Schedule 3 (Pricing Schedule) paragraph 2.1 (Pricing for Fixed Cost after volume discount) of the Contract which contained the new Fixed Cost or volumes for Year 2 was set out in Annex 4 of the said Deed of Variation.

3. The Authority has requested further variations of some of the terms and conditions of the Contract as agreed in a letter from the Authority to the Contractor dated 5th April 2018 regarding "CQC's Requirements for Year 3 of the Experts by Experience Contract for Central Region" and the Contractor has agreed to these terms. The terms to be varied are as follows:

a. amendment of the terms of the Contract to ensure compliance with the new General Data Protection Regulation ("GDPR");
b. variation of the Contract to extend it from 1st June 2018 to 31st January 2019;
c. amendment of Volumes Requirements for Year 3 contained in Schedule 1- Specification;
d. amendment of Fixed Costs for Year 3 contained in Schedule 3 – Pricing Schedule;
e. variation of costs for shorter specific inspection events contained in Paragraph 2.2 of Schedule 3; and
e. further amendments of the KPIs contained in Schedule 4 of the Contract which was varied in the Deed of Variation dated 9th October 2017.

4. The Contractor has agreed to provide these services as part of the Services under the terms and conditions of the Contract.

NOW IT IS AGREED between the Authority and the Contractor as follows:

1. The provisions of paragraphs (a) – (o) inclusive, (t) and (u) of this Deed of Variation shall have effect from the date of communication agreed by the parties or 25th May 2018, whichever is earlier.

2. In accordance with clause F8 of the Contract, the Contract Period is further extended by seven months from 1st June 2018 to 31st January 2019. For the avoidance of doubt the Contract shall expire automatically on 31st January 2019, unless it is otherwise terminated in accordance with the provisions of the Contract or otherwise lawfully terminated.

3. The provisions of paragraphs (p), (q) (r) and (s) of this Deed shall have effect from 1st June 2018.

4. The Contract is varied as set out in the table below;

Paragraph	Clause	Variation
a	Definition is amended **"Data Controller**, **Data Processor** and **Personal Data** shall have the same meaning as set out in the Data Protection Act 1998"	This definition is amended to read as follows: **"Data Controller, Data Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer** shall each have the same meaning given in the GDPR"
b	Definition added:	This definition is inserted into the agreement: **"Data Loss Event** means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach"
c	**Definition deleted** **"DPA** means the Data Protection Act 1998 and any subordinate legislation made under such Act from time to time together with any guidance and/or codes of practice issued by the	

	Information Commissioner or relevant government department in relation to such legislation"	
d	Definition added:	This definition is inserted into the agreement: **"Data Protection Legislation** means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; (ii) the DPA 2018 to the extent that it relates to the processing of Personal Data and privacy; (iii) all applicable Law about the processing of Personal Data and privacy;"
e	Definition added:	This definition is inserted into the agreement: **"Data Protection Impact Assessment** means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;"
f	Definition added:	This definition is inserted into the agreement: **"Data Subject Access Request** means a request made by or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access his or her Personal Data;"
g	Definition added:	This definition is inserted into the agreement: **"GDPR"** means the General Data Protection Regulation (*Regulation (EU) 2016/679*)"
h	Definition added:	This definition is inserted into the agreement: **"LED"** means Law Enforcement Directive *(Directive (EU) 2016/680)*;
i	Definition added:	This definition is inserted into the agreement: **"Personal Data** (as defined in the Data Protection Legislation) which is Processed by the Contractor or any Sub-contractor on behalf of the Authority or a Central Government Body pursuant to or in

		connection with this Contract"
j	Definition added:	This definition is inserted into the agreement: **"Processing** has the meaning given to it in the Data Protection Legislation but, for the purposes of the Contract, it shall include both manual and automatic processing and "Process" and "Processed" shall be interpreted accordingly;"
k	Definition added:	This definition is inserted into the agreement; **"Sub-processor** means any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement";
l	Clause B9.1A added;	This clause is inserted into the agreement; "The Contractor shall ensure that its controlled architecture and environment used to process or store Authority Data will be certified to the NCSC Cyber Essentials Plus certification scheme."
m	Clause E1 deleted;	The entire text of Clause E1 is deleted and replaced with Annexe 1 of this Deed of Variation
n	Clauses E6.6 – E6.10 are added	These clauses is inserted into the Contract "E6.6 The Contractor shall, as an enduring obligation during the Contract Period, use the latest versions of anti-virus definitions available from an industry accepted anti-virus software vendor to check for and delete Malicious Software from the ICT Environment. E6.7 Notwithstanding clause E6.5, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of the Authority Data, assist each other to mitigate any losses and to restore the provision of Services to their desired operating efficiency and the Contractor shall immediately take all reasonable steps necessary to: (a) minimise the extent of actual or potential harm caused by any Breach of Security; (b) remedy such Breach of Security to the extent

		possible and protect the integrity of the Services to the extent within its control against any such Breach of Security or attempted Breach of Security; (c) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and (d) as soon as reasonably practicable provide the Authority with full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority. E6.8 Any cost arising out of the actions of the Parties taken in compliance with clause E6.6 shall be borne by the Parties as follows: (a) by the Contractor where the Malicious Software originates from the Contractor Software, the Third Party Software or the Authority Data (whilst the Authority Data was under the control of the Contractor); and (b) by the Authority if the Malicious Software originates from the Authority Software or Authority Data (whilst the Authority Data was under the control of the Authority). E6.9 The Contractor controlled architecture and environment used to process or store Authority Data will be certified to the NCSC Cyber Essentials Plus certification scheme. E6.10 The Contractor shall be liable for, and shall indemnify the Authority against all Losses suffered or incurred by the

		Authority and/or any third party arising from and/or in connection with any Breach of Security or attempted Breach of Security (to the extent that such Losses were not caused by any act or omission by the Authority)."
o	Clause G1.3 amended	Clause G1.3 is amended to read as follows: G1.1 "Liability under clauses B9.4, E1.18, E6.8, G1.1, **Error! Reference source not found.** and **Error! Reference source not found.** shall be unlimited. Liability under clauses **Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.** shall be subject to the limitation of liability set out in clause G1.4."
p	Annex 1 - Volumes and Events to Contract contained in Schedule 1 "Specification" to be deleted	Annex 1 - Volumes and Events to Contract contained in Schedule 1 "Specification" to be deleted and replaced with Annex 2 of this Deed
q	Table 1 of Paragraph 2.1 "Fixed Costs" of Schedule 3 "Pricing Schedule" to be deleted	Table 1 of Paragraph 2.1 "**Fixed Costs**" of Schedule 3 "Pricing Schedule" to be deleted and replaced with Annex 3 of this Deed of Variation.
r	Table 2 "**Inspection and other Event costs**" of Paragraph 2.2 of Schedule 3 "Pricing Schedule" - : is deleted Schedule	Table 2 of Paragraph 2.2 of Schedule 3 – Pricing Schedule - **Inspection and other Event costs:** is deleted is replaced with Annex 4 of this Deed of Variation.
s	Schedule deleted	Schedule 4 deleted and replaced within Annex 5 of this Deed of Variation
t	Schedule added	Schedule 6A added Annex 1A of this Deed of Variation.
u	Schedule added	"Schedule 14 – Processing, Personal Data and Data Subject" is added as Annex 6 of this Deed of Variation.

5. The Contract shall expire automatically on 31st January 2019 (in accordance with the provisions of clause A2 of the Contract) unless it is otherwise terminated in accordance with the provisions of the Contract, or otherwise lawfully terminated, or extended under clause F8.

6. Other than the above variations the Contract shall remain in full force and effect as varied by this Deed and the terms of the Contract shall have effect as though the variations contained in this deed had been originally contained in the Contract.

7. This Contract shall be subject to English law in all respects (including formation) and shall be construed and interpreted in accordance with English law and shall be subject to the jurisdiction of the Courts of England.

EXECUTED as a Deed by the Parties on the date which first appears in this instrument:

[redacted]

EXECUTED as a Deed by

The common seal of
CHOICE SUPPORT was hereunto affixed
in the presence of:

[redacted]

ANNEX 1 OF THIS DEED OF VARIATION

E1 Data Protection Act

E1.1 The Contractor shall (and shall procure that its entire Staff) comply with any notification requirements under Data Protection Legislation and both Parties will duly observe all their obligations under Data Protection Legislation which arise in connection with the Contract.

E1.2 The Contractor will, in conjunction with the Authority, in its own right and in respect of the Services, shall ensure it will be compliant with the provisions of the GDPR and Data Protection Legislation.

E1.3 The Contractor shall designate and will provide the Authority with the contact details of its data protection officer where this position is required by the Data Protection Legislation or other designated individual with responsibility for data protection and privacy to act as the point of contact for the purpose of observing its obligations in this Clause E1.

E1.4 If the Contractor is Processing Personal Data as a Data Processor for the Authority, the Contractor shall:

(a) Prior to the processing of any Personal Data under this Contract and where requested by the Authority provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment ("DPIA"). Such assistance may, at the discretion of the Authority include (but not be limited to):

i. A systematic description of the envisaged processing operations and the purpose of the processing;

ii. An assessment of the necessity and proportionality of the processing operations in relation to the Services;

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

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

(b) implement and maintain appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected including the measures as are set out in Clause B9 (Cyber Security) and Schedule 6 (Security Requirements, Policy and Plan).

(c) Process the Personal Data only in accordance with Schedule 14 and/or written instructions from the Authority (which may be specific instructions or instructions of a general nature) as set out in the Contract or as otherwise notified by the Authority unless the Contractor is required to do so otherwise by Law. If it is so required, the Contractor shall promptly notify the Authority before processing the Personal Data unless prohibited by Law;

(d) Process the Personal Data only to the extent and in such manner as is necessary for the provision of the Contractor's obligations under the Contract or as is required by Law or any Regulatory Body;

(e) Keep a record of all categories of processing activities carried out on behalf of the Authority, containing;

i) the categories of processing carried out on behalf of the Authority;

ii) where applicable, any transfers of Personal Data to Restricted Countries or an international organisation.

(f) Ensure that it has in place Protective Measures, which have been reviewed and approved by the Authority as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

(g) take all reasonable steps to ensure the reliability and integrity of any Contractor's Personnel who have access to the Personal Data and ensure that the Contractor's Personnel:

a. do not process Personal Data except in accordance with this Agreement (and in particular Schedule 14);

b. are aware of and comply with the Contractor's duties under this Clause E1 and Clause E3(Confidential Information);

c. are subject to appropriate confidentiality undertakings with the Contractor or any relevant Sub-contractor;

d. 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 Authority or as otherwise permitted by this Contract; and

e. have undergone adequate training in the use, care, protection and handling of personal data (as defined in the Data Protection Legislation);

(h) not disclose or transfer the Personal Data to, or allow the processing of Personal Data by any Sub-Contractor and/or Affiliates for the provision of the Services without Approval;

(i) not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:

(i) the Authority or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Authority;
(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Contractor 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 Authority in meeting its obligations); and
(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Authority with respect to the processing of the Personal Data;

(j) at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data;

(k) notify the Authority within 48 hours if it:

a. receives from a Data Subject (or third party on their behalf):

i. a Data Subject Access Request (or purported Data Subject Access Request);

ii. a request to rectify, block or erase any Personal Data; or

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

b. considers that any of the Authority's instructions from the Authority infringe the Data Protection Legislation;

c. receives any Regulator Correspondence or any other any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract; or

d. 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

e. is required by Law to commit an act or omission to that would, but for Clause E1.10, constitute a breach of this Clause E1;

f. becomes aware of a Data Loss Event

(l) The Contractor's obligation to notify under Clause E1.4 (k) shall include the provision of further information to the Authority in phases, as details become available.

E1.4A Notwithstanding the provisions of clauses E1.1 and E1.4, where the Contractor is Processing Personal Data for the Authority, the parties acknowledge that the Authority is the Data Controller and the Contractor is the Data Processor. The Authority shall set out the scope, nature and purpose of the Processing by the Contractor, the duration of the Processing and the types of Personal Data and the categories of Data Subject in the form appended hereto in Schedule 14 – Processing, Personal Data and Data Subject.

E1.5 Taking into account the nature of the processing, the Contractor shall provide the Authority with full co-operation and assistance (within the timescales reasonably required by the Authority) in relation to either Party's obligations under Data Protection Legislation or any complaint, communication or request made as referred to in Clause E1.4(k), including by promptly providing:

a. the Authority with full details and copies of the complaint, communication or request;

b. where applicable, such assistance as is reasonably requested by the Authority to enable the Authority to comply with the Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation; and

c. the Authority, on its request, with any Personal Data it holds in relation to a Data Subject;

d. assistance as requested by the Authority following any Data Loss Event; and

e. as requested by the Authority with respect to any request from the Information Commissioner's Office (ICO), or any consultation by the Authority with the Information Commissioner's Office;

E1.6 The Contractor shall, if requested by the Authority, provide a written description of the measures that it has taken and technical and organisational security measures in place, for the purpose of compliance with its obligations pursuant to this Clause E1 and provide to the Authority copies of all documentation relevant to such compliance including, processing records, procedures, guidance, training and manuals.

E1.7 The Contractor shall allow the Authority (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit, in accordance with clause E9 (Audit), the Contractor's Data Processing activities (and/or those of Staff) and comply with all reasonable requests or directions by the Authority to enable the Authority to verify and/or procure that the Contractor is in full compliance with its obligations under the Contract;

E1.8. The Contractor shall not Process or otherwise transfer any Personal Data in or to any Restricted Country without the Authority's prior written consent. If, after the Effective Date, the Contractor or any Sub-contractor wishes to Process and/or transfer any Personal Data in or to any Restricted Country, the Contractor shall, in seeking consent, submit such information as the Authority's shall require in order to enable it to consider the request and acknowledges that such consent may be given subject to conditions which will, if appropriate, be incorporated into this Contract at the Contractor's cost and expense using the Change Control Procedure.

E1.9 The Contractor will notify the Authority immediately, and in any event no later than 12 hours, after becoming aware of a Data Loss Event, in particular the notification will be made regardless as to whether or not the Contractor has established any unauthorised access or other harm has actually arisen from the event. Notification must not be delayed for the purpose of establishing the effects of an identified Data Loss Event. In particular the Contractor will;

i) when notifying the Authority of a Data Loss Event will describe the nature of the event including the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

ii) Cooperate fully with any Authority investigation into the Data Loss Event including but not limited to the causes and effects (actual or potential);

iii) provide immediate access to the Contractor's premises and systems for the purposes of any Authority investigation under Clause E1.9 ii above

iv) Take all necessary actions to remedy the causes or adverse effects of the Data Loss Event and to ensure the protection of Personal Data from any further loss. Where the contractor reasonably considers that immediate action is required to ensure the protection of personal data, or to prevent or mitigate a serious risk of harm, damage or loss to data subjects arising from a Data Loss Event, they may take such action without requiring prior authorisation from the Authority circumstances where it is not reasonably possible to seek or obtain such authorisation in a timely manner;

v) Not make any public statement of any kind without the prior Approval of the Authority;

vi) Where appropriate, provide all assistance necessary to enable the Authority to fulfil its obligations to notify the Information Commissioner within 72 hours after becoming aware of the Data Loss Event; and

vii) notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.

E1.10 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause E1. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(a) the Authority determines that the processing is not occasional;
(b) the Authority determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
(c) the Authority determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

E1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:

(a) notify the Authority in writing of the intended Sub-processor and processing;
(b) obtain the written consent of the Authority;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause E1 such that they apply to the Sub-processor; and

(d) provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

E1.12 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

E1.13 The Authority may, at any time on not less than 30 Working Days' notice, revise this clause 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 this Agreement).

E1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

E1.15 At the end of the Term or earlier termination of this Contract, at the Authority's request, the Contractor shall delete or return all Personal Data to the Authority and delete any copies of such Personal Data except where required to retain any copies by Law.

E1.16 The Contractor shall comply at all times with Data Protection Legislation and shall not perform its obligations under the Contract in such a way as to cause the Authority to breach any of its applicable obligations under the Data Protection Legislation.

E1.17 The Contractor shall use its reasonable endeavours to assist the Authority to comply with any obligations under the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Authority to breach any of the Authority's obligations under the Data Protection Legislation to the extent the Contractor is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

E1.18 The Contractor shall indemnify the Authority on a continuing basis against any and all Losses incurred by the Authority arising from the Contractor's Default under this Clause E1 and/or any failure by the Contractor or any Sub-Contractor to comply with their respective obligations under Data Protection Legislation.

E1.19 Nothing in this Clause E1 shall be construed as requiring the Contractor or any relevant Sub-contractor to be in breach of any Data Protection Legislation.

E1.20 The provision of this clause E1 applies during the Contract Period and indefinitely after its expiry.

ANNEX 1A OF DEED OF VARIATION

SCHEDULE 6A

Security Requirements, Policy and Plan

INTERPRETATION AND DEFINITION

For the purposes of this Schedule 6A, unless the context otherwise requires the following provisions shall have the meanings given to them below:

"Breach of Security" means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor System, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract.

"Contractor Equipment" means the hardware, computer and telecoms devices and equipment supplied by the Contractor or its Sub-Contractor (but not hired, leased or loaned from the Authority) for the provision of the Services;

"Contractor Software" means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services and which is specified as such in Schedule 6A.

"ICT" means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony.

"Protectively Marked" shall have the meaning as set out in the Security Policy Framework.

"Security Plan" means the Contractor's security plan prepared pursuant to paragraph 3 an outline of which is set out in an Appendix to this Schedule 6A.

"Software" means Specially Written Software, Contractor Software and Third Party Software.

"Specially Written Software" means any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this Contract.

"Third Party Software" means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software and which is specified as such in Schedule 6A.

1. INTRODUCTION

This Schedule 6A covers:

1.1 principles of security for the Contractor System, derived from the Security Policy Framework, including without limitation principles of physical and information security;

1.2 wider aspects of security relating to the Services;

1.3 the creation of the Security Plan;

1.4 audit and testing of the Security Plan; and

1.5 breaches of security.

2. PRINCIPLES OF SECURITY

2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of Authority Data.

2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:

2.2.1 is in accordance with Good Industry Practice and Law;

2.2.2 complies with Security Policy Framework; and

2.2.3 meets any specific security threats to the Contractor System.

2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):

2.3.1 loss of integrity of Authority Data;

2.3.2 loss of confidentiality of Authority Data;

2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;

2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Contractor in the provision of the Services;

2.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.

2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority.

3. SECURITY PLAN

3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule 6A.

3.2 A draft Security Plan provided by the Contractor as part of its bid is set out herein.

3.3 Prior to the Commencement Date the Contractor will deliver to the Authority for approval the final Security Plan which will be based on the draft Security Plan set out herein.

3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause I2 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 may be unreasonably withheld or

delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.4 shall be deemed to be reasonable.

3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

3.5.1 the provisions of this Schedule 6A;

3.5.2 the provisions of Schedule 1 relating to security;

3.5.3 the Information Assurance Standards;

3.5.4 the data protection compliance guidance produced by the Authority;

3.5.5 the minimum set of security measures and standards required where the system will be handling Protectively Marked or sensitive information, as determined by the Security Policy Framework;

3.5.6 any other extant national information security requirements and guidance, as provided by the Authority's IT security officers; and

3.5.7 appropriate ICT standards for technical countermeasures which are included in the Contractor System.

3.6 The references to Quality Standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such Quality Standards, guidance and policies, from time to time.

3.7 If there is any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authorised Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001 or other equivalent policy or procedure, cross-referencing if necessary to other schedules of the Contract which cover specific areas included within that standard.

3.9 The Security Plan shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule 6A.

4. AMENDMENT AND REVISION

4.1 The Security Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:

4.1.1 emerging changes in Good Industry Practice;

4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes;

4.1.3 any new perceived or changed threats to the Contractor System;

4.1.4 changes to security policies introduced Government-wide or by the Authority; and/or

4.1.5 a reasonable request by the Authority.

ANNEX 1 OF SCHEDULE 6A: BASELINE SECURITY REQUIREMENTS

1. HIGHER CLASSIFICATIONS

1.1 The Contractor shall not handle Authority Data and information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Contractor shall seek additional specific guidance from the Authority.

2. END USER DEVICES

2.1 When Authority Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Authority Data and services must be under the management authority of the Authority or Contractor and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Contractor devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2).

Where the guidance highlights shortcomings in a particular platform the Contractor may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Contractor wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

3.1 The Contractor and Authority recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Contractor must be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all times.

3.2 The Contractor shall agree any change in location of data storage, processing and administration with the Authority in advance where the proposed location is outside the UK. Such approval shall not be unreasonably withheld or delayed unless specified otherwise in this Agreement and provided that storage, processing and management of any Authority Data are only carried out offshore within:

3.2.1 the European Economic Area (EEA);

3.2.2 in the US if the Contractor and or any relevant Sub-Contractor have Signed up to the US-EU Privacy Shield Register; or

3.2.3 in another country or territory outside the EEA if that country or Territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the EU Commission.

3.3 The Contractor shall:

3.3.1 provide the Authority with all Authority Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Authority Data in the event of the Contractor ceasing to trade;

3.3.3 securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Authority Data held by the Contractor when requested to do so by the Authority.

4. NETWORKING

4.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

4.2 The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY ARCHITECTURES

5.1 The Contractor shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Authority Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) the Contractor shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification(http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor).

5.3 The Contractor shall ensure that its controlled architecture and environment used to process or store Authority Data will be certified to the NCSC Cyber Essentials Plus certification scheme.

6. PERSONNEL SECURITY

6.1 Supplier Contractor Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 Contractor shall agree on a case by case basis Contractor Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Authority Data.

6.3 Contractor shall prevent Contractor Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

6.4 All Contractor Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information

ANNEX 2 OF SCHEDULE 6A: SECURITY POLICY

20180521 CQC
Security Policy.doc

Annex 2 of this Deed of Variation

Schedule 1 – Specification – New Volumes for Year 3

The following is replacing Schedule 1 – Specification, Annex 1 – Volumes and Events to Contract for Year 3

Central Region

Contract Year 3	Central
ASC-R	1534
ASC-C	651
NHS Acute	23
MH NHS	-
PMS	12
IH	-
MH Act	24
MH NHS, IH, IH MH & SMU	120
Registration	12
Total Inspections	2,376
Total Engagements	**144**

ANNEX 3 OF THIS DEED OF VARIATION

SCHEDULE 3 – PRICING FOR NEW FIXED COST VOLUMES FOR YEAR 3

Paragraph 2.1

Fixed Costs

Table 1

Central	Current Year 3	Year 3 agreed
[redacted]		

ANNEX 4 OF THIS DEED OF VARIATION

SCHEDULE 3 – PRICING FOR NEW INSPECTION AND OTHER EVENT COSTS

Paragraph 2.2

Table 2.

Sector	EXE Type	Price 1 day	Supporter	Price 2 days	Supporter
NHS ACUTE & IH	D/FCD	[redacted]			
	OP/FCD				
	PS				
	MH				
	SM				
	CYP				
	MAT				
NHS MH & IH	MH	[redacted]			
	MHD				
	SM				
	D / FCD				
	OP / FCOP				
	LD				

COLUMN 1 Service Requirement	COLUMN 2 Reporting Measurement	COLUMN 3 Reporting Frequency	COLUMN 4 Performance Target	COLUMN 5 Performance Points allocated to KPI	COLUMN 6 Required Action Notice Level	COLUMN 7 Corrective Action Notice Level
7. Provide within one Month of receipt from the Authority of the quarterly allocation of Events the indicative named Expert by Experience for all such Events	Percentage of Events which the Contractor has provided an indicative named Expert by Experience within one Month of receipt from the Authority of the quarterly allocation of Events	Quarterly	75%	3	74 – 66%	65%
8. Maintain a pipeline of resource of Experts by Experience to meet the volume requirements of Experts by Experience as set in out in the Tender response	Percentage of Experts by Experience employed or engaged by the Contractor (by category) against the Authority's requirements for that category as set out in Annex 1 of the Specification	Quarterly	100%	3	99% - 81%	80%
9. Have a credible and sustainable training methodology and programme that supports the ongoing Quality Standards of the Services	Percentage of Experts by Experience that are deployed by the Contractor within 2 Months of successful completion of all induction training	Quarterly	90%	3	89% - 71%	70%
10. Have a credible means of evaluating the performance of an Expert by Experience of an Event	Percentage of Experts by Experience that meet all of the quality standards set out in Annex 6 of the Specification	Quarterly	100%	2	99% - 81%	80%
11. Have a policy on how the Contractor or its supply chain will interact with and support the	A survey of Experts by Experience is completed by all Experts by Experience employed or engaged by the	Every six (6) Months	85%	2	84% -66%	65%

COLUMN 1 Service Requirement	COLUMN 2 Reporting Measurement	COLUMN 3 Reporting Frequency	COLUMN 4 Performance Target	COLUMN 5 Performance Points allocated to KPI	COLUMN 6 Required Action Notice Level	COLUMN 7 Corrective Action Notice Level
Experts by Experience on a regular basis to maintain their wellbeing	Contractor					
	Proportion of Experts by Experience that give an overall 'satisfied' (or above) response to the Contractor's survey. *Note: The content of such survey to be agreed in advance with the Authority. This survey will also be used to test other KPIs.*	Every six (6) Months	75%	2	71% - 61%	60%
12. Establish a viable strategy that seeks to minimise the carbon footprint and environmental impact of the Services delivered	Percentage of public transport of used as a proportion of transport method of attendance to the Events (excluding those Experts by Experience who are unable to access public transport) *Note: Assumed anyone deemed to be unable to access public transport will have an objective assessment articulating this and appropriate support plan that still seeks to minimise environmental impact*	Every six (6) months	60%	1	59% - 41%	40%

COLUMN 1 Service Requirement	COLUMN 2 Reporting Measurement	COLUMN 3 Reporting Frequency	COLUMN 4 Performance Target	COLUMN 5 Performance Points allocated to KPI	COLUMN 6 Required Action Notice Level	COLUMN 7 Corrective Action Notice Level
C. BUSINESS MANAGEMENT						
13. Payment of sub-contractors or the Experts by Experience within 30 days from the receipt of a valid invoice	Percentage of sub-contractors or the Experts by Experience paid within 30 days from the receipt of a valid invoice	Monthly	98%	3	97% - 91%	90%
14. Attendance at meetings	Percentage of attendance at all meetings as required for contract management requirements as set out within the Specification	Monthly	100%	3	99% - 91%	90%
15. OVERALL KPI PERFORMANCE SCORE	The overall performance across all of the above KPIs will be measured by calculating the number of Performance Points awarded to each KPI (in line with the Performance Points allocation set out in Column 5 for the relevant KPI). Performance Points will only be awarded to a KPI if the Contractor achieves the Performance Target (set out in	Monthly	**Monthly Performance Points Allocation:** between 13-15 Performance Points **Quarterly Performance Points Allocation:** between 26-	N/A	**Monthly Performance Points Allocation:** between 13-10 Performance Points **Quarterly Performance Points Allocation:**	**Monthly Performance Points Allocation:** Below 10 Performance Points **Quarterly Performance Points Allocation:** Below 23

COLUMN 1 Service Requirement	COLUMN 2 Reporting Measurement	COLUMN 3 Reporting Frequency	COLUMN 4 Performance Target	COLUMN 5 Performance Points allocated to KPI	COLUMN 6 Required Action Notice Level	COLUMN 7 Corrective Action Notice Level
	Column 4) and no Performance Points will be awarded to a KPI where the performance of a KPI falls below the Performance Target (set out in Column 4). Where the relevant reporting Month does not fall on a Quarter of the Contract Year (and therefore only KPIs with a Monthly reporting frequency are reported), the Monthly Points Allocation as set out in this row 15 shall apply Where the relevant reporting Month falls on a Quarter Month of the Contract Year but not on a Half Year (and therefore KPIs with a Monthly and Quarterly reporting frequency will be measured) the Quarterly Points Allocation as set out in this row 15 shall apply. Where the relevant reporting Month falls on a Quarter Month of the Contract Year but not on a Half Year (and therefore KPIs with a Monthly and Quarterly reporting frequency will be measured) the Quarterly Points Allocation as set out in this row		28 Performance Points **Half Year Performance Points Allocation:** between 35-37 Performance Points		between 23-26 Performance Points **Half Year Performance Points Allocation:** between 30-35 Performance Points	Performance Points **Half Year Performance Points Allocation:** Below 30 Performance Points

COLUMN 1 Service Requirement	COLUMN 2 Reporting Measurement	COLUMN 3 Reporting Frequency	COLUMN 4 Performance Target	COLUMN 5 Performance Points allocated to KPI	COLUMN 6 Required Action Notice Level	COLUMN 7 Corrective Action Notice Level
	15 shall apply.					

ANNEX 6 OF THIS DEED OF VARIATION

SCHEDULE 14 - PROCESSING, PERSONAL DATA AND DATA SUBJECT

PROCESSING, PERSONAL DATA AND DATA SUBJECTS

For purposes of this Schedule, Contractor shall have the same meaning as Supplier and the Authority shall have the same meaning as the Client or Customer as defined in the Agreement.

1. The Contractor shall comply with any further written instruct ions with respect to processing by the Authority.

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	Experts by Experience
Duration of the processing	25/05/2018 – 31/01/2019
Nature and purposes of the processing	The personal data being processed by the contractor is for the purpose of carrying out the terms of the Experts by Experience (ExE) contract. ExE are employed by the Contractor to assist the Authority on inspections by speaking to people who use services, their family carers, relatives and friends and gathering their views and experiences of care. The ExE methodology stipulates that ExE should not identify named individuals in the information they pass to inspectors either in the form of hand-written notes or typed reports. The Authority also requests ExE take part in in co-production and engagement events and ongoing monitoring activities via the Contractor.

The Contractor will use ExE personal details to contact them about participating in work for the Authority, and will also pass their personal details to the Authority in the form of a Pen Portrait to effect liaison between inspectors and other Authority staff for the purposes of carrying out the above activities. CQC will retain and destroy any ExE information in line with our own retention periods which are referred to in our published information Asset Register.

The Contractor will also use the personal data of the ExE to invite them to communicate with them in relation to human resources and payroll issues, and to invite them to training and development events to assist them in carrying out their role.

Where complaints are raised in relation to the activities of ExE by employees of the Authority, people who use services, service providers or other members of the public, which may include safeguarding issues, the Authority will investigate such matters in partnership with the Contractor, using the minimum amount of personal data necessary.

Where the Authority knows of individuals that represent a risk to people who use services, the Authority will advise the Contractor of this fact should the individual apply to take part in the programme.

Choice Support has issued an ExE Employee privacy notice to each Expert by Experience in the central region.

We have a named data protection officer.

General Data Protection Regulation (GDPR)

Choice Support has a process for reminding and checking with individual Experts by Experience when to destroy securely any data they have linked to their involvement with an event.

once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	all notes and contact details relating to the inspection when the final inspection report is published, or after six weeks of the inspection event, unless otherwise requested by the inspector in relation to enforcement activity. Where this is the case the inspector will require the ExE to securely send them their contemporaneous notes, in which case the destruction of the data becomes the responsibility of the inspector. CQC will retain and destroy any ExE information in line with our own retention periods which are referred to in our published information Asset Register. The exit management and transition checklist links into the exit strategy and shared risk log. The authority and the supplier have interchanging roles from processor to controller throughout this process. GDPR principals will be adhered to throughout the contract exit plan. This will be in compliance with clause H7 in the contract - Exit Management.