CHANGE CONTROL

Contract Change Note

Contract Change Note Number	CCN001
Contract Reference Number & Title	CQC ICTC 723 – Contract for the Provision of Support, Maintenance and Hosting for CQC's National Resource Planning Solution
Variation Title	Extension of Contract Period and Variation to terms and conditions of the Original Contract
Number of Pages	15

WHEREAS

CACI LIMITED ('the Contractor') and the **CARE QUALITY COMMISSION** ('the Authority') entered into a Contract for the provision of Support, Maintenance and Hosting for CQC's National Resource Planning Solution dated 7 July 2017 (the "Contract") and now wish to amend the Contract.

IT IS AGREED as follows:

1. The Contract shall be amended as set out in this Change Control Notice:

Change Requestor / Originator	Care Quality Commission	
Summary of Change	The Authority wishes to extend the Contract Period in accordance with clause 1.3. Furthermore, the Authority wishes to vary the terms of the Contract by invoking the provisions of clause 23. The specific contract amendments required by this Contract Change Note are set out in detail in **Annex 1.**	
Reason for Change	To extend the Contract Period from 1 July 2018 to 30 June 2019, to put the Contract in line with the General Data Protection Legislation and as a result of independent audit review.	
Revised Contract Price	Original Contract Value	£943,862
	Contract Change Note CCN 001	£242,788
	New Contract Value	£1,186,650
Revised Payment Schedule	Please see Schedule 2 of Annex 1.	
Revised Specification	N/A	

Revised Contract Period	The Contract Period is hereby extended commencing on 1 July 2018 to 30 June 2019.
Change in Contract Manager(s)	The contract will continue to be managed by Gavin Kennedy
Other Changes	N/A

2.   Save as herein amended all other terms of the Contract shall remain effective.

3.   This Change Control Notice shall take effect on 1 July 2018 save for the Variations made to put the Contract in line with the General Data Protection Legislation and security clauses which shall be effective from 25 May 2018.

SIGNED ON BEHALF OF THE AUTHORITY	SIGNED ON BEHALF OF THE CONTRACTOR
Signature:	Signature
Name:	Name:
Position:	Position:
Date:	Date:

Annex 1

Amendments to terms and conditions of Contract

The following new definitions shall be added to Clause 1 in chronological order. Any and all references in the Original Contract to the following definitions below shall be deleted and replaced accordingly.

1 Definitions and Interpretation

"Agreement" means this Contract;

"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;

"DPA or Data Protection Legislation" means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; and (ii) the DPA 2018 to the extent that it relates to the processing of Personal Data and privacy;

"Data Protection Impact Assessment" means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

"Data Subject 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;

"DPA" means the Data Protection Act 2018 and any subordinate legislation made under that Act;

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

"LED" means Law Enforcement Directive *(Directive (EU) 2016/680)*;

"Loss" means any losses, costs, charges, expenses, interest, fees (including reasonable legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, charges, fines, damages, destruction, adverse judgments, orders or other sanctions and the term **Losses** shall be construed accordingly

"Processor Personnel" means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub Processor engaged in the performance of its obligations under this Agreement;

"Protective Measures" means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it including those outlined in Schedule 6 (Security Policy and Plan).

"Sub-processor" means any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement;

Clause 4 shall be deleted in its entirety and replaced by the following:

4   Protection of Information

4.1   The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor. The only processing that the Processor is authorised to do is listed in Schedule 10 by the Controller and may not be determined by the Processor.

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

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

   (a)   a systematic description of the envisaged processing operations and the purpose of the processing;

   (b)   an assessment of the necessity and proportionality of the processing operations in relation to the Services;

   (c)   an assessment of the risks to the rights and freedoms of Data Subjects; and

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

4.4   The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

   (a)   process that Personal Data only in accordance with Schedule 10, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

   (b)   ensure that it has in place Protective Measures, which are appropriate to protect against a Personal Data Breach, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

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

   (c)   ensure that:

      (i)   the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 10);
      (ii)   it takes all reasonable steps to ensure the reliability and integrity of any Processor

Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

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

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

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

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

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

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

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

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

4.5 Subject to clause 4.6, the Processor shall notify the Controller immediately if it:

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

(b) receives a request to rectify, block or erase any Personal Data;

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

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;

(e) 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

(f)　becomes aware of a Personal Data Breach.

4.6　The Processor's obligation to notify under clause 4.5 shall include the provision of further information to the Controller in phases, as details become available.

4.7　Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 4.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a)　the Controller with full details and copies of the complaint, communication or request;

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

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

(d)　assistance as requested by the Controller following any Personal Data Breach; and

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

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

(a)　the Controller determines that the processing is not occasional;

(b)　the Controller 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; or

(c)　the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

4.9　The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor. The audit rights in this Clause 4.9 shall be subject to the Controller or the Controller's Representative; (i) giving prior reasonable written notice of any such audit; (ii) exercising its right to audit no more than once a year during the term of this Contract; (iii) conducting any such audit during the Processor's normal business hours; (iv) complying with the Processor's confidentiality, IT security and health and safety policies and procedures; and (v) causing minimal disruption to the Processor's business when conducting any such audit.

4.10　Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

4.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:

     (a)   notify the Controller in writing of the intended Sub-processor and processing;

     (b)   obtain the written consent of the Controller;

     (c)   enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 4 such that they apply to the Sub-processor; and

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

4.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

4.13 The Controller 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 Contract.

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

4.15 Subject always to Clause 15.4.2 (Liability) the Processor shall indemnify the Controller on a continuing basis against any and all Losses incurred by the Controller resulting from a third party claim (the ICO shall be considered to be a third party) that arises from the Processor's breach of its obligations under this Clause 4 subject to the Controller :

(a) promptly notifying the Processor of any claim;

(b) not making any admission in relation to any claim without the Processor's prior written approval;

(c)the Processor having control of the defence and any settlement;

(d)providing all reasonable assistance to the Processor as it may request in relation to the defence of the claim;

(e) consulting with the Processor throughout the course of the claim and keeping the Processor fully updated in relation to the claim at all times; and

(f)mitigating its costs, losses and damages.

Any and all losses, damages and costs paid or payable by the Controller to any third party resulting from the Processor's breach of this Clause 4 (including Clause 4A) must be pursued under this indemnity.

4.16 Nothing in this Clause 4 shall be construed as requiring the Processor or any relevant Sub-processor to be in breach of any Data Protection Legislation.

4.17 The provision of this Clause 4 applies during the Contract Period and indefinitely after its expiry.

New clause 4A is added:

4A   Security

4A.1   The Authority shall be responsible for maintaining the security of the Authority's Premises in accordance with its standard security requirements. The Contractor shall comply with all security requirements of the Authority while on the Authority's Premises, and shall ensure that all Staff comply with such requirements.

4A.2   The Contractor shall ensure that the Security Plan produced by the Contractor fully complies with Schedule 6 (Security Requirements, Policy and Plan).

4A.3   The Contractor shall comply, and shall procure compliance of its Staff, with Schedule 6 (Security Requirements, Policy and Plan).

4A.4   The Authority shall notify the Contractor of any changes or proposed changes to Schedule 6 (Security Requirements, Policy and Plan).

4A.5   The Contractor controlled architecture and environment used to process or store Authority Data will be certified to the NCSC Cyber Essentials Plus certification scheme or its equivalent.

Clause 15.4.2 of the Contract shall be deleted in its entirety and replaced with the following:

15.4.2 for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Authority Data or the Authority Personal Data or any copy of such Authority Data, caused by the Contractor's default under or in connection with the indemnity pursuant to Clause 4.15 shall in no event exceed £5,000,000;

Clause 15.4.6 of the Contract shall be deleted in its entirety and replaced with 'Not Used'.

Schedule 2 is deleted in its entirety and replaced by the following:

SCHEDULE 2 – PRICING

As per the details supplied in CACI's proposal 'CACI_CQC_NRPS_Contract_Extension_2018_v2' dated 22nd May,2018. CQC is committing to the following two estimates embedded below. Additionally, any further services procured during this extension will be as per CACI's rate card included in the same proposal document at section 4.

Care Quality Commission (CQC) Cygnum ASM renewal for the period 1st July 2018 to 30th June 2019

Estimate Reference: E00112020CQC

CACI Ltd - Enterprise Systems Business Unit, IMS (hereafter referred to as CACI) is pleased to provide this estimate for the costs of the services outlined below.

Customer: Care Quality Commission (CQC)
Address: T70 Payables F175
              Phoenix House
              Topcliffe Lane
              Wakefield
              WF3 1WE

CACI consider some of the material contained in this proposal to be highly commercially sensitive and would therefore ask Care Quality Commission (CQC) to respect the confidential nature of this document. Notwithstanding the transparency required for any democratic process, CACI ask that this response is not to be copied to any third party without the written agreement of CACI.

COMMERCIAL IN CONFIDENCE

DATE:	VERSION STATUS	AUTHOR:	APPROVED BY:
15 Jun 2018	Initial Document	J Strong	O Watson

Validity
All prices quoted are valid for 30 days from latest version date of this document, which is 15 July 2018.

Acceptance
A written order is required before this estimate can be actioned by CACI.

Services
All charges are subject to VAT. Where services are charged per diem, the daily charge rate is fixed and is also subject to VAT. Please note that all day rates are exclusive of expenses, which are charged at cost, and/or 48p per mile car travel where appropriate. This estimate is provided subject to existing Terms and Conditions agreed between CACI and Care Quality Commission (CQC). This proposal is an estimate of effort subject to further clarification of requirements.

Fee Type: Fixed Fee
This is a fixed price. The charge will not be dependent on the amount of time taken to complete the work. In agreeing to this fixed price you are agreeing to be charged the total estimate value.

Invoicing Basis: Bill Planning
The charges will be invoiced on a quarterly basis or an agreed planned basis. Where charges are not quarterly, see additional notes for details. Where an annual licence fee is estimated, charges will be made once the software is installed.

Annual Licence Fee

Annual Support and Maintenance Fees are due 30 days from commencement of User Acceptance Testing or when the software is loaded into the Live Environment, whichever is soonest.

Lead Time: 4 weeks
The lead time is the time taken from the receipt of your purchase order to the time that CACI can start the work or service. Lead time starts when the order is received and accepted by CACI.

TASK DESCRIPTION	DAILY RATE	ESTIMATE OF EFFORT		Total
		Workstage	Days	
Cygnum (including NRPS Phase 2 & 3) ASM renewal for the period 1st July 2018 to 30th June 2019	n/a	SUPPORT AND MAINTENANCE FEE	n/a	
RPI Uplift 3.3% Cygnum	n/a	SUPPORT AND MAINTENANCE FEE	n/a	
Third Party Rocket support	n/a	THIRD PARTY ALF	n/a	
Hosting	n/a	THIRD PARTY ALF	n/a	

Total Days Effort   **0**

Annual Support & Maintenance	**£147243.40**
Total Implementation Cost	**£0.00**
Grand Total	**£147243.40**

Care Quality Commission (CQC)
Ongoing Assistance Scheme (OAS) - July 2018 to June 2019
Estimate Reference: E00112021CQC
CACI Ltd - Enterprise Systems Business Unit, IMS (hereafter referred to as CACI) is pleased to provide this estimate for the costs of the services outlined below.

Customer: Care Quality Commission (CQC)
Address: T70 Payables F175
                       Phoenix House
                       Topcliffe Lane
                       Wakefield

CACI consider some of the material contained in this proposal to be highly commercially sensitive and would therefore ask Care Quality Commission (CQC) to respect the confidential nature of this document. Notwithstanding the transparency required for any democratic process, CACI ask that this response is not to be copied to any third party without the written agreement of CACI.

COMMERCIAL IN CONFIDENCE

DATE:	VERSION STATUS	AUTHOR:	APPROVED BY:
15 Jun 2018	**Initial Document**	**J Strong**	**O Watson**

Validity
All prices quoted are valid for 30 days from latest version date of this document, which is 15 July 2018.

Acceptance
A written order is required before this estimate can be actioned by CACI.

Services
All charges are subject to VAT. Where services are charged per diem, the daily charge rate is fixed and is also subject to VAT. Please note that all day rates are exclusive of expenses, which are charged at cost, and/or 48p per mile car travel where appropriate. This estimate is provided subject to existing Terms and Conditions agreed between CACI and Care Quality Commission (CQC). This proposal is an estimate of effort subject to further clarification of requirements.

Fee Type: Fixed Fee
This is a fixed price. The charge will not be dependent on the amount of time taken to complete the work. In agreeing to this fixed price you are agreeing to be charged the total estimate value.

Invoicing Basis: Bill Planning
The charges will be invoiced on a quarterly basis or an agreed planned basis. Where charges are not quarterly, see additional notes for details. Where an annual licence fee is estimated, charges will be made once the software is installed.

Lead Time: 4 weeks
The lead time is the time taken from the receipt of your purchase order to the time that CACI can start the work or service. Lead time starts when the order is received and accepted by CACI.

TASK DESCRIPTION	DAILY RATE	ESTIMATE OF EFFORT		Total
		Workstage	Days	
Ongoing Assistance Scheme (OAS) - July 2018 to June 2019	■■■■	IMPLEMENTATION	■■■■	■■■■
		Total Days Effort		■■■■

	Total Implementation Cost	£55080.00
	Grand Total	£55080.00

New Schedule 10 shall be added as follows:

SCHEDULE 10 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The contact details of the Controller's Data Protection Officer are: Nimali de Silva, Care Quality Commission, 3rd Floor, Buckingham Palace Road, London SW1W 9SZ.

2. The contact details of the Processor's Data Protection Officer are: Raj Afghan

3. The Processor shall comply with any further reasonable and lawful written instructions with respect to processing by the Controller.

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

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor in accordance with Clause 4.1.
Subject matter of the processing	The primary data entities that Cygnum processes are Organisational, Personal and Inspection related data.
Duration of the processing	25 May 2018 until the expiration of the Contract Period or early termination of the Contract.
Nature and purposes of the processing	Cygnum is an enterprise resource planning system that helps CQC schedule and resource it's inspection activity. To

	facilitate this, Cygnum stores the personal data of substantive staff , casual workers (such as Specialist Advisors and Bank Inspectors) and agency workers (such as Experts by Experience). It does this by allowing CQC Inspectors to create inspection records in Cygnum (either manually or automatically using defined frequency business rules). Inspectors then "request" specific resources to support their inspection which notifies various scheduling teams in CQC. These scheduling teams then use algorithms in Cygnum to find the most suitable resources to fill the role (in the case of Specialist Advisors and Bank Inspectors) or the data is exported and sent to support organisations (for Experts by Experience). Once suitable resources have been identified they are asked to confirm their attendance and upon doing so some of their personal details (such as name, phone number, email address, roles/specialisms) are made available to the Inspector in order for them to make contact ahead of the inspection. The algorithm used to find suitable resources considers factors such as availability, roles/specialisms, travel distance, conflicts of interest and DBS status. Post-inspection it is possible for CQC staff to provide feedback on resources that attended an inspection to support any required performance management.
Type of personal data	Cygnum stores the following data (mastered in ESR): • ESR Number • Names (Title, Forenames, Surnames, Preferred Names) • CQC Hire Date

	- Work email (CQC staff), personal email (non-CQC staff) - Work phone (CQC staff), personal phone (non-CQC staff) - Address – Town/City, County and Postcode (not First Line of Address) - ESR Assignment Data – ID, Start/End Date, Contract Type, Line Manager, FTE, Hours per Week, Job Title, Cost Centre, Directorate, Region, Patch, Grade - Specialism s - DBS Status - Professional Registration details Cygnum also records (as master records) the following personal data: - Availability data - Conflicts of Interest - Timesheets - Annual Leave Entitlements/Bookings
Categories of Data Subject	Staff: All CQC Staff - Specialist Advisors - Bank Inspectors Organisations (mastered in CRM): - Registered Managers - Nominated Individuals - Any other persons associated with an organisation. Other - CRM Contact Records (members of the public etc.) - Experts by Experience

Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	There are currently no plans for destruction of data in Cygnum. We are currently discussing with KIM colleagues what this should look like and CACI are looking to develop additional functionality to support automatic/manual data destruction.