CONTRACT CHANGE NOTE (CCN)

CR NO.: CQC ICTC 560/561	OVER-ARCHING CONTRACT TITLE: Provision of Digital Hosting and Managed Service	COMMENCEMENT DATE OF CCN : 27/01/2017
PROJECT: Provision of Digital Hosting and Managed Service	TYPE OF CHANGE: Short-term extension	EXPIRY DATE OF CCN: 30/09/2017

DETAILED DESCRIPTION OF CONTRACT CHANGE AND DETAILS OF ANY RELATED CONTRACT CHANGES:

To enable a period of technological understanding and alignment in relation to the Customer's on-going hosting requirements the Customer requires a short-term continuation of the existing Digital Hosting and Support provision.

The extension will comprise of a continuation of the Services outlined within the Over-arching Contract. Details of the Scope of Works to be undertaken can be located within Annex A and is a continuation of the over-arching Contract.

In addition to the continuation of Service, the following provisions will apply to this Contract Change Note:

- The Customer will have the option to terminate the services on 1st July 2017. The Customer will provide no less than 30 days written notice in the event the Customer wishes to enforce this option here-in known as 'Break-point'.

- The Support days classed as 'Ad-Hoc' within the Support element of the over-arching Contract will be reduced from [redacted]; it is forecasted to be proportioned as [redacted] for OLS and 3 days for Public however this split is not defined. All other elements of the service provision including SLA's remain as-per the over-arching Contract.

- The Supplier understands and accepts that the Customer may request the provision of an Exit Plan. In the event this is required by the Customer, full details of the requirements will be issued to the Supplier for review and is to be agreed by both Parties. Full details of any request for an Exit Plan will be provided to the Supplier no later than 30 days prior to the required date.

- "Clause CO9.1 is deleted and replaced with the following:

  - CO- 9.1 This Call-Off Agreement shall take effect on the Effective Date and shall expire on:
  - CO- 9.1.1 the date specified in paragraph 1.2 of the Order Form; or
  - CO- 9.1.2 twenty four (24) Months after the Effective Date, whichever is the earlier, unless terminated earlier pursuant to the Clause CO-9; or
  - CO-9.1.3 where the Call-Off Agreement is extended in accordance with CO-9.1.4, the end of the period of extension.
  - CO-9.1.4The Customer shall have the right to extend this Call-Off Agreement by

periods up to twelve (12) Months in total. Such request will be made in writing by the Customer to the Supplier stating the period of extension required. For the avoidance of doubt, the Supplier shall continue to provide the Ordered G-Cloud Services until the end date of any period of extension in accordance with CO-10.2 and the Customer shall continue to pay the Charges in accordance with CO-13.

- CO-9.1.4.1 The Customer may, during any extension period under CO-9.1.4 request transitional services for a specified period of the extension. Such a request will be made in writing to the Supplier, giving not less than 3 months' written notice of the Customer's transitional requirements and shall be in compliance with CO-21.

If no such extension is requested by the Customer in accordance with this CO-9.1.4 the Call-Off Agreement shall expire pursuant to CO-9.1.1 or CO-9.1.2"

This Contract Change Note is effective from 27th January 2017 and comprises the written notice required by CO-9.1.4, that the Customer requires an extension of the Call-Off Agreement so that it will expire on: 30th September 2017.
The Customer requires the Supplier to continue to provide the Ordered G-Cloud Services in accordance with the Call-Off Agreement. The Customer reserves the right to request a further extension of time and to request transitional services on accordance with CO-9.1.4.1.

This Contract Change Note is subject to the Terms and Conditions of the over-arching Agreement.

KEY MILESTONE DATE(S):

Contract Change Note Milestones

Milestone	Anticipated Completion Date
1. Potential enforcement of Contract Break-point	1st July 2017
2. Confirmation regarding whether Exit Provision required	31st August 2017
3. End of Contract Change Note and handover of Exit Plan if requested	30th September 2017

PROPOSED ADJUSTMENT TO THE CHARGES RESULTING FROM THE CONTRACT CHANGE:

There are no proposed changes to the price of the over-arching Contract and the requirements for invoicing will remain as per the over-arching Contract.

For a period of 8 months continuation of service the price of the Agreement will be: **183,476 (ex VAT).**

This figure comprises of:

- Hosting and support and Maintenance [redacted]

Anticipated payments will be as follows:

Feb17: [redacted]
Mar17
Apr17:
May17
Jun17: [redacted]
Jul17: [redacted]
Aug1
Sep17

- Application Support allocation [redacted]

Anticipated payments will be as follows:

[redacted]

Payment will be made in equal monthly payments in arrears for the work undertaken within the month prior.

DETAILS OF PROPOSED ONE-OFF ADDITIONAL CHARGES AND MEANS FOR DETERMINING THESE (E.G. FIXED PRICE OR COST-PLUS BASIS):

N/A- see above.

SIGNED ON BEHALF OF THE CUSTOMER:	SIGNED ON BEHALF OF THE SUPPLIER:
Signature: [redacted]	Signa [redacted]
Name:_	Nam
Position:	Posit

Date:____________________	Date:_[redacted]______

Annex A- CQC Requirements

1. Executive Summary

CQC requires the continuation of the existing Service Provision detailed within the over-arching Agreement 'CQC ICTC 560/561'. This Annex provides a high-level summary of the Customer's requirements for the Contract Change Note which is also replicated within the over-arching Agreement and will be delivered in-line with the Supplier's original proposal.

Hosting services are required by CQC to:

- Provide information to the public via an online presence (public website)
- Provide online transactions for providers (Provider Portal)
- Support third-party digital services
- Publish our statutory register of services.

Managed services are required by CQC to:
:

- Provide transition and hosting of the CQC online presence
    - **CQC website** – CCN service to commence 27th January 2017
    - **CQC online communities** - CCN service to commence 27th January 2017
    - **CQC Provider Portal** – CCN service to commence 27th January 2017
- Implement the new services before the corresponding transition period of the contracts end
- Provide an uninterrupted service during the process of transition to the new service, and thereafter

- Provide best value for money, secure and performant infrastructure solution for hosting CQC websites
- Provide a platform that allows CQC to deploy and maintain software

2. Current Solution Overview

CQC's main public facing website – www.cqc.org.uk

The purpose of this website is to disseminate information to the public about the standard of care provided in hospitals, care homes, dental surgeries and other registered care providers. A large part of the website is a directory of 100K+ care services, which is updated currently on a daily basis.

- The site receives approximately 4.7 million page views a month – a figure that's steadily growing.
- The site runs off a database-driven content management system (CMS) known as Drupal 7, in combination with several layers of caching and the EdgeCast Content Delivery Network (CDN). A full list of software currently used to support the delivery of the website is listed in Appendix A.
- The Drupal CMS reads from two distinct databases: its own Drupal database, and a separate MongoDB database. All directory information is stored in MongoDB in a key-value structure.
- Data is fed via an external Enterprise Service Bus, built using MuleSoft ESB.
- The search facility is powered by an external Solr service.
- The website uses an external messaging service ElasticEmail to send email alerts to members of the public.
- The site uses multiple database and web servers, and multiple layers of software and hardware caching to achieve its required performance.
- Neither the general public nor providers or care services are able to log into the site (i.e. the vast majority of the site's users are anonymous).

CQC online communities websites

These are two websites are dedicated to interacting with the public (https://communities.cqc.org.uk/public/) and healthcare providers (https://communities.cqc.org.uk/provider/) and gathering their views on subjects related to how CQC operates.

- The two websites can be accessed by authenticated users only. The public website has 2580 and the provider website has 9303 active users (as of June 2015).
- The websites were built using the Drupal 7 Commons distribution. They have then been configured and slightly customised. Both sites share the same codebase and have separate databases. There is a caching layer, but no CDN.
- The websites contain sensitive data and require IL2 hosting.

- The websites use an external messaging service ElasticEmail to send emails to their users.

CQC Provider Portal– https://services.cqc.org.uk/

The Provider Portal is a web-based platform that allows the providers that CQC regulates to carry-out transactions online. CQC regulates approximately 30,000 providers who submit around 420,000 forms per annum. These transactions fall into broadly into two main types:

1) Registration variations
2) Statutory notifications

The Portal has been used by GPs since October 2013, to carry out variations to their registration. High-volume statutory notifications went live in April and Provider Portal accounts are currently being rolled out to other sectors. This should be completed by the end of 2015.

The Portal is built on Drupal 7 and integrates with internal systems via a Java/PostgreSQL-based middleware layer (out of scope for this proposal).

Infrastructure Requirements

CQC Volumetric Specification

CQC require the ability to add and remove infrastructure within 10 working days as required due to increase or decrease in volumetrics

ID	Requirement	CQC website	Online communities	Provider Portal
IR1.1	Number of documents*	[redacted]	[redacted]	[redacted]
IR1.2	Number of image files *	[redacted]	[redacted]	[redacted]
IR1.3	Number of video files *	[redacted]	[redacted]	[redacted]
IR1.4	Number of audio files *	[redacted]	[redacted]	[redacted]
IR1.5	Average total site visits per month **	[redacted]	[redacted]	[redacted]
IR1.6	Peak site visits per day **	[redacted]	[redacted]	[redacted]
IR1.7	Average Page Impressions per month **	[redacted]	[redacted]	[redacted]
IR1.8	Number of unique editors	[redacted]	[redacted]	[redacted]
IR1.9	Average Search Requests per month **	[redacted]	[redacted]	[redacted]
IR1.10	CDN traffic requirement per month **	[redacted]	[redacted]	[redacted]
IR1.11	Backup tape storage requirement per month **	[redacted]	[redacted]	[redacted]
IR1.12	Number of Provider Portal user accounts activated (total)***	[redacted]	[redacted]	[redacted]
IR1.13	Number of Provider Portal online transactions per month****	[redacted]	[redacted]	[redacted]

** on 15 July 2015*

*** For April/May/June 2015*

**** Provider Portal accounts are currently being rolled out to all sectors. The first figure is for number of accounts at the end of June 2015. The second figure is an estimate of the number of accounts expected by 31 December 2015 and the third figure is the maximum currently anticipated.*

***** Monthly online transaction. The first figure is for June 2015, the second is an estimate for December 2015 and the third figure is the likely maximum number of transactions.*

For up-to and including OS Level:

Required Service Availability and Continuity (up to and including OS level)

ID	Availability Metric	Monthly Target
IR2.1	Live environments and data - the service utilised by an End User, i.e. citizen or a business including all data	99.95%
IR2.2	Contributed Environment and data - the service used by editors, developers in order to manage Content and/or transactions	99.8%
IR2.3	Planned maintenance and releases to the solution shall be completed outside of UK business hours and without disruption to the users	99.8%
IR2.4	Non-Live environments to be available during standard business hours	99.0%
IR2.5	Non-Live environments to be available outside standard business hours	95.0%
IR2.6	In the event of any compromise to the full service (e.g. in the case of invoking a disaster recovery service) the full service shall be restored within 12 hours	100%

Service Performance

These conform to the standard measures as implemented by www.newrelic.com

ID	Performance Metric	Monthly Target
IR3.1	App server Apdex T-value 0.5 seconds	0.96

IR3.2	Browser Apdex T-value 7 seconds	0.98

Environments Infrastructure

Provision of hardware, software and support up to and including OS level

ID	Requirement	CQC website	Online communities	Provider Portal
IR4.1	A hosted Drupal 7 platform with the following instances: a) Development environment b) Test environment c) Production environment d) Disaster recovery environment e) Staging environment f) Additional testing environment	a, b, c, d	a, c	a, b, c, d, e, f
IR4.2	The solution must provide a high availability: a) MySQL database b) MongoDB database	a, b	a	a, b
IR4.3	The solution must provide a caching service: a) CDN cache	a, b, c	b, c	N/A

	b) Page furniture cache (e.g. Nginx) c) HTML and search cache (e.g. Varnish)			
IR4.4	Disaster recovery - The solution must provide a high availability	H	H	H
IR4.5	Load balancing - There should be no single point of component failure, so load balancing should be deployed where necessary to balance requests.	H	H	H
IR4.6	The sites must continue to integrate with: a) Elastic Email b) Axis12 Find service (Solr) c) CQC ESB d) Google maps e) Google places f) Google geo-code g) Checkbox h) OpenAM	a, b, c, d, e, f	a	c, h

Data Centre

ID	Requirement

IR5.1	Hosting environment must be certified to IL2 for Online communities and Provider Portal
IR5.2	Data Centre to have classification of at least Tier III from the Uptime Institute or alternative comparable classification
IR5.3	All elements of the hosting solution must physically exist within the European Union
IR5.4	External and internal access to environments should be via firewalls

Migration

ID	Requirement
IR6.1	Migration design required - The Supplier must utilise as much as, if not all, software configuration and development (code base) from the previous solution, ideally in a "lift and shift" approach. Redevelopment and bespoking must be kept to a minimum and must be expressly identified in the solution
IR6.4	Security testing
IR6.5	Documentation - Technical Architecture required Transparency on hosting resources and design will be shared with CQC

Development Features

The ability for CQC to perform these tasks in all environments is required

ID	Requirement
IR7.1	Ability to SHH to all environments

Above OS Level:

Service Availability and Continuity (above OS level)

ID	Availability Metric	Monthly Target
IR2.1	Live environments and data - the service utilised by an End User, i.e. citizen or a business including all data	99.95%
IR2.2	Contributed Environment and data - the service used by editors, developers in order to manage Content and/or transactions	99.8%
IR2.3	Planned maintenance and releases to the solution shall be completed outside of UK business hours and without disruption to the users	99.8%
IR2.4	Non-Live environments to be available during standard business hours	99.0%
IR2.5	Non-Live environments to be available outside standard business hours	95.0%
IR2.6	In the event of any compromise to the full service (e.g. in the case of invoking a disaster recovery service) the full service shall be restored within 12 hours	100%

Service Performance

These conform to the standard measures as implemented by www.newrelic.com

ID	Performance Metric	Monthly Target
IR3.1	App server Apdex T-value 0.5 seconds	0.96
IR3.2	Browser Apdex T-value 7 seconds	0.98

Environments Infrastructure

Provision of software and support above OS level is in scope of this tender

ID	Requirement	CQC website	Online communities	Provider Portal
IR4.1	A hosted Drupal 7 platform with the following instances: g) Development environment h) Test environment i) Production environment j) Disaster recovery environment k) Staging environment l) Additional testing environment	a, b, c, d	a, c	a, b, c, d, e, f
IR4.2	The solution must provide a high availability:	a, b	a	a, b

	c) MySQL database d) MongoDB database			
IR4.3	The solution must provide a caching service: d) CDN cache – CQC already has a direct arrangement with EdgeCast e) Page furniture cache (e.g. Nginx) f) HTML and search cache (e.g. Varnish)	a, b, c	b, c	N/A
IR4.4	Disaster recovery - The solution must provide a high availability	H	H	H
IR4.5	The sites must continue to integrate with: i) Elastic Email j) Axis12 Find service (Solr) k) CQC ESB l) Google maps m) Google places n) Google geo-code o) Checkbox p) OpenAM	a, b, c, d, e, f	a	c, h

Migration

ID	Requirement
IR6.1	Migration design required - The Supplier must utilise as much as, if not all, software configuration and development (code base) from the previous solution, ideally in a "lift and shift" approach. Redevelopment and bespoking must be kept to a minimum and must be expressly identified in the solution
IR6.2	Deployment support required
IR6.3	System integration testing
IR6.4	Security and Penetration testing

Development Features

The ability for CQC to perform these tasks in all environments is required

ID	Requirement
IR7.1	Ability to copy databases from Production to non-Production environments and vs versa
IR7.2	Ability to download databases and assets to create local dev environments
IR7.3	Have full access to all code repositories and branches
IR7.4	Ability to deploy code to all environments
IR7.5	Ability to SHH to all environments

3. SERVICE MANAGEMENT REQUIREMENTS

Service and Support KPI's

ID	Category	Service Level Measurement	Monthly Service Level Target
SM1.1	Incident and Problem Management	Incidents logged through a Service Desk channel acknowledged immediately	100%
SM1.2		Severity 1 incidents resolved within 2 hours of logging the incident. During the investigation updates to be provided every 15 min and root cause of incident reported within 24 hours of incident resolution	100%
SM1.3		Severity 2 incidents resolved within 6 business hours of logging the incident	100%
SM1.4		Severity 3 incidents resolved within 2 business days of logging the incident	95%
SM1.5		Severity 4 incidents resolved or closed (and corresponding problem record created) within 5 business days of logging the incident	95%
SM1.6		All incidents to be resolved within 20 business days	100%
SM1.7	Service Management	Service reports and plans circulated in accordance with defined schedule unless otherwise agreed between the parties	100%
SM1.8		Service requests logged through a Service Desk channel acknowledged within 30 min	100%
SM1.9		Impact assessment for Service Requests delivered within 3 business days	100%
SM1.10		Service requests completed and closed within	100%

		timescales agreed as part of Impact Assessment process	

Security

ID	Requirement
SM2.1	Supplier must hold a current ISO27001 certificate with the British Standards Institution
SM2.2	All employees with access to IL2 data on the hosting environment must have undergone appropriate security screening that can be evidenced if requested

Support

ID	Requirement
SM3.1	**Infrastructure monitoring** Provision of detailed server side monitoring, tracking resource consumption and ability to set alarms and send emails and text messages when configurable thresholds are met.
SM3.2	Ticketing system to raise and track requests/issues
SM3.3	Performance testing - The solution must be able to allow for meaningful and consistent performance testing
SM3.1	Support for out of hours releases required
SM3.2	**Web monitoring** Provision of log monitoring, ability to set alarms and send emails and text messages when configurable thresholds are met and/or events occur. Monitoring service must monitor all components of the solution, including Web, DB, Varnish, external connections (Solr, ESB). Full access to reporting must be enabled.

Service Management Plans Required at Commencement of Service

ID	Purpose
SM4.1	Service Continuity - To show what processes the Supplier has in place to safeguard the continuity of the business
SM4.2	Availability - To detail how the availability SLA(s) will be met including reference to Disaster Recovery arrangements and how this would support the attainment of the SLA.
SM4.3	Capacity - To detail how the Supplier will monitor and manage capacity, in terms of people, ability to meet traffic volumes, etc.
SM4.4	Change Management - To detail how the Supplier will manage the integration of changes to services so that the organisation has minimal disruption

SM4.5	Incident Escalation - To detail the process for escalating incident severity – e.g. who to contact and how. Also to detail how CQC will be kept updated.
SM4.6	Severity 1 incident - To detail how severity 1 incidents will be managed to ensure the incident resolution SLA can be achieved

Service Management Reports

ID	Name of report / Frequency	Purpose
SM5.1	Release schedule / Updated weekly	Details of all service fixes to be implemented and release dates
SM5.2	Major incidents action point log / Monthly and ad hoc based on request	Detail action points raised at major incident reviews and tracks them to resolution
SM5.3	Monthly incident report / Monthly	Details all open incidents with details of progress towards resolution
SM5.4	Service requests status report / Monthly and ad hoc	Details status of all open Service Requests and intended implementation

Support time

[redacted]vill be provided to maintain the solution.
[redacted] will be provided for ad-hoc support requests. Those days will have to be transferable to the following month if unused.

Any request by CQC that is deemed outside of this scope should be approved first before executed and changed for.

Incident Management Categorisation

The following is the required categorisation of incidents; suppliers should state any deviations from these in the service management offered by the solution.

Severity 1: Impact = Critical

Functional	Total or partial apparent loss or significant degradation of the performance of the solution
	A large number of Users or End Users are unable to access the solution or part of the solution
Security	A security breach has been detected and remains critical until its impact is known
	A new or unknown virus has been detected and remains critical until its impact is known and the Incident is re-classified if appropriate
	Targeted attack
	Non-targeted attack
	Loss of data affecting the security of the network, infrastructure of systems
	Theft/loss of cryptography equipment or media
	DoS/DDos – successful
	AV alert/quarantine – widespread
	Loss of public online service
	Unauthorised access
	Damaging unauthorised changes to system hardware
	Phishing (fraud involving misuse of branding).

Severity 2: Impact = Serious

Functional	A small number of Users or End Users are unable to use the solution or part of the solution as normal and they are carrying out time critical business activities
	Performance is significantly degraded but the Solution is still usable.
Security	DoS/DDos – unsuccessful
	Network monitoring alert
	Employee abuse of privileges or security policy (e.g. emailing login credentials).

Severity 3: Impact = Minor

Functional	A small number of Users or End Users are unable to use the solution or part of the solution as normal. No time critical business activities are affected
	Performance is slightly degraded but the Solution is still usable
Security	AV alert/quarantine – single

Severity 4: Impact = Low

Functional	The Solution or part of the Solution does not perform as expected by the User but does not prevent the User from performing time critical business activities and the Solution or part of the Solution does not fail. Processing completes as required. A workaround is available and/or planned. No critical processing is affected. These Incidents are characterised as 'irritants' and may be closed as Incidents and logged as a corresponding problem
Security	None defined

APPENDIX A

Current Hosting Infrastructure

Public Site

[redacted]

Community Sites

[redacted]

Provider Portal

[redacted]

System Diagrams

Public site

[redacted]