SCHEDULE 4 – CHANGE CONTROL

Contract Change Note

Contract Change Note Number	CCN-1
Contract Reference Number & Title	CQC AM 139 Lot 2 – National Stakeholder Sentiment Survey extension
Variation Title	Extension
Number of Pages	111

WHEREAS **COMMUNICATE RESEARCH LIMITED** (" the Contractor" and the **CARE QUALITY COMMISSION** ("the Authority") entered into a Contract for the provision of CQC AM 139 Public Research Lot 2 – National Stakeholder Sentiment Survey dated 02/05/2017 (the "Original Contract") and now wish to amend the Original Contract

IT IS AGREED as follows

1. The Original 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 Term of the Contract in accordance with Clause 1.3 until 31 March 2019. In addition, the Authority wishes to vary the terms and conditions of the Contract to put it in line with the new General Data Protection Regulation (GDPR) and incorporate security clauses as a result of an independent audit review by invoking the provisions of Clause F6. The specific contract amendments required by this Contract Change Note are set out in detail in **Annex 1**.
Reason for Change	The purpose for this Contract Change Notice is the continuation of service by ComRes to benchmark stakeholder awareness and sentiment from a representative sample of national charities which will allow CQC to improve performance and to ensure work has maximum impact and value for money. It is also being varied due to the change in data protection legislation and as a

	result of independent audit review.	
Revised Contract Price	Original Contract Value	£ 11,375
	Contract Change Note CCN-1	£ 11,375
	New Contract Value	£22,750 ex VAT
Revised Payment Schedule	The payment schedule will remain the same as the original contract whereby ComRes will be paid monthly in arrears via purchase order for all work completed.	
Revised Specification	There is no change to the specification as CQC's requirements remain the same as the original contract.	
Revised Contract Period	The contract change notice will run until 31/03/2019	
Change in Contract Manager(s)	[redacted]	
Other Changes	No further changes are required.	

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

3. This Change Control Notice shall take effect from the date on which both the Authority and the Contractor have communicated acceptance of its terms. The variation on the terms and conditions in Annex 1 shall take effect on 25 May 2018.

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

Annex 1

Amendments to terms and conditions of the Contract

Effective 25 May 2018, the following amendments shall apply

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

A1 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;

"Data Loss Event" means any event that results, or may result, in unauthorised access to Personal Data held by the Processor 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;

"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;

"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 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;

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

"Law" means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Contractor is bound to comply;

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

"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;

"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 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;

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

Clause E2 shall be deleted and replaced by the following:

E2 Data Protection & Privacy

The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor. The only processing that the Supplier is authorised to do is listed in Schedule 14 by the Customer and may not be determined by the Supplier.

E2.2 The Supplier shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

E2.3 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.

E2.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule 14, 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 Data Loss Event, 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 Data Loss Event;

(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 Agreement (and in particular Schedule 14);

(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 Agreement; 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 Agreement unless the Processor is required by Law to retain the Personal Data.

E2.5 Subject to clause E2.6, the Supplier shall notify the Controller immediately if it:

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

(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 Data Loss Event.

E2.6 The Processor's obligation to notify under clause E2.5 shall include the provision of further information to the Controller in phases, as details become available.

E2.7 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 13.5 (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 Data Loss Event;

(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.

E2.8 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.

E2.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

E2.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

E2.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, 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 13 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.

E2.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

E2.13 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 Agreement).

E2.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Supplier amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

E2.15 The Processor shall indemnify the Controller on a continuing basis against any and all Loss(es) incurred by the Controller arising from the Processor's Default under this Clause E2 and/or any failure by the Contractor or any Sub-Contractor to comply with their respective obligations under Data Protection Legislation.

E2.16 Nothing in this clause E2 shall be construed as requiring the Processor or any relevant Sub-processor to be in breach of any Data Protection Legislation.

E2.17 The provision of this clause E2 applies during the Contract Period and indefinitely after its expiry.

Contractor wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

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.

NETWORKING

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).

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.

SECURITY ARCHITECTURES

New Clause E7.7A shall be added as follows:

E7.7A The Contractor controlled architecture and environment used to process or store Authority Data will be certified to the NCSC Cyber Essentials Plus certification scheme.

New Clause G1.2A shall be added as follows:

G1.2A Liability under Clauses E2.18 and E7.8 shall be limited to the maximum regulatory fine imposable for breach of Data Protection Legislation.

Clause G1.3 shall be amended as follows:

G1.3 Insert " and G1.2A" after "clause G1.1".

The following new annexes to Schedule 8 shall be added:

SCHEDULE 8 - SECURITY REQUIREMENTS, POLICY AND PLAN

ANNEX 1: BASELINE SECURITY REQUIREMENTS

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.

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

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.

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).

PERSONNEL SECURITY

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

The 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.

The 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.

All Contractor Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

Where the Contractor or Sub-Contractors grants increased ICT privileges or access rights to Contractor Personnel, those Contractor Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

IDENTITY, AUTHENTICATION AND ACCESS CONTROL

The Contractor shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Contractor shall retain an audit record of accesses.

AUDIT AND MONITORING

The Contractor shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include:

Contractor wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

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.

NETWORKING

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).

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.

SECURITY ARCHITECTURES

Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

The Contractor and the Authority shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

The Contractor shall retain audit records collected in compliance with this Paragraph 0 for a period of at least 6 months.

ANNEX 2: SECURITY POLICY

ATTACHED SEPERATELY

New Schedule 14 shall be added as follows:

SCHEDULE 14 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The contact details of the Controller's Data Protection Officer are: Nimali de Silva

2. The contact details of the Processor's Data Protection Officer are: Mark Ellis

3. The Processor shall comply with any further 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 Customer is the Controller and the Contractor is the Processor in accordance with Clause 13.1.
Subject matter of the processing	National Stakeholder Sentiment Survey: research into what our national VCS stakeholders think of CQC.
Duration of the processing	25 May 2018 until expiration or early termination of the contract
Nature and purposes of the processing	This contract involves an external supplier holding qualitative interviews with 25 VCS organisations. The results of this research are then fed back to CQC.
Type of personal data	Work e-mail addresses, work telephone numbers
Categories of Data Subject	VCS organisations
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state	Contact details can be deleted by the supplier as soon as the research is over (by December 2018 at the latest)

law to preserve that type of data