RM6098 Framework Schedule 6a (Short Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	CQC TDI 002
THE BUYER:	Care Quality Commission
BUYER ADDRESS	Care Quality Commission Citygate Gallowgate Newcastle upon Tyne NE1 4PA
THE SUPPLIER:	Softcat PLC
SUPPLIER ADDRESS:	Fieldhouse Lane, Marlow, SL7 1LW
REGISTRATION NUMBER:	02174990
DUNS NUMBER:	397333253
SID4GOV ID:	N/A

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 10 October 2025.
It's issued under the Framework Contract with the reference number RM6098 for the provision of Technology Products & Associated Services.

CALL-OFF LOT(S):
Lot 3 Software

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6098
3. Framework Special Terms

4. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6098
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)

5. CCS Core Terms (version 3.0.11) as amended by the Framework Award Form
6. Joint Schedule 5 (Corporate Social Responsibility) RM6098

CALL-OFF SPECIAL TERMS
The following Special Terms are incorporated into this Call-Off Contract:

1. This Call-Off Contract incorporates the MAXQDA End User Licence Agreement (the 'EULA') set out below:

MAXQDA Terms

2. As payment is an agreed one-time payment upfront in advance, no automatic renewal of this Contract shall take place.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF START DATE: 10 November 2025

CALL-OFF EXPIRY DATE: 09 November 2028

CALL-OFF INITIAL PERIOD: Three (3) years

CALL-OFF DELIVERABLES

[redacted]

LOCATION FOR DELIVERY
There is no physical delivery required.

DATES FOR DELIVERY

10/11/2025

WARRANTY PERIOD
The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be 90 days.

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is [redacted]

CALL-OFF CHARGES

[redacted]

£33,621.58 Excl VAT (£40,345.90 Incl VAT)

PAYMENT METHOD
Upfront in advance.
Invoice – Method of Payment is BACS to [redacted]

BUYER'S INVOICE ADDRESS:
Care Quality Commission
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4PA

BUYER'S AUTHORISED REPRESENTATIVE
[redacted]
Care Quality Commission
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4PA

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

SUPPLIER'S CONTRACT MANAGER
[redacted]

KEY SUBCONTRACTOR(S)
MAXQDA

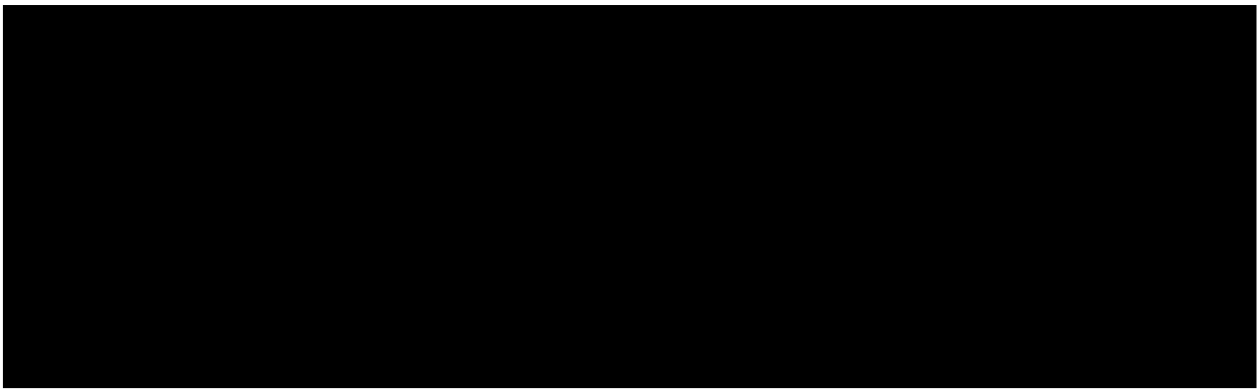
COMMERCIALLY SENSITIVE INFORMATION
N/A

GUARANTEE
Not applicable

IN WITNESS of which this Contract has been duly executed by the Parties the day and year first before written

SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Authorised Signatory:



SIGNED for and on behalf of **Softcat PLC**

Authorised Signatory 1:

Authorised Signatory 2:

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	**[delete** as applicable: CCS / Buyer**]** (**"CCS" "the Buyer"**) And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete** as applicable: CCS / Buyer**]**

Signature .....
Date .....
Name (in Capitals) .....
Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature	.....
Date	.....
Name (in Capitals)	.....
Address	.....

Joint Schedule 3 (Insurance Requirements)

1. **The insurance you need to have**
    1. The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("Additional Insurances") and any other insurances as may be required by applicable Law (together the “Insurances”). The Supplier shall ensure that each of the Insurances is effective no later than:
        1. the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
        2. the Call-Off Contract Effective Date in respect of the Additional Insurances.
    2. The Insurances shall be:
        1. maintained in accordance with Good Industry Practice;
        2. (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
        3. taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
        4. maintained for at least six (6) years after the End Date.
    3. The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.
2. **How to manage the insurance**
    1. Without limiting the other provisions of this Contract, the Supplier shall:
        1. take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
        2. promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
        3. hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.
3. **What happens if you aren’t insured**
    1. The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
    2. Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the

relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. **Evidence of insurance you must provide**

1. The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. **Making sure you are insured to the required amount**

1. The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. **Cancelled Insurance**

1. The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
2. The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

1. The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.
2. Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
3. Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
4. Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible

under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the Framework Start Date in accordance with this Schedule:

1.1 Professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

1.2 Public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

1.3 Employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000) – all Lots.

1.4 Product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000) – all Lots.

Joint Schedule 4 (Commercially Sensitive Information) – Not Applicable

1. **What is the Commercially Sensitive Information?**

1. In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
2. Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
3. Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
	[insert date]	[insert details]	[insert duration]

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default:	[**Guidance:** Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the [Revised] Rectification Plan:	[**add** date (minimum 10 days from request)]		
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default	[**add** cause]		
Anticipated impact assessment:	[**add** impact]		
Actual effect of Default:	[**add** effect]		
Steps to be taken to rectification:	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[**add** reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

a. "Controller" in respect of the other Party who is "Processor";
b. "Processor" in respect of the other Party who is "Controller";
c. "Joint Controller" with the other Party;
d. "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller and may not otherwise be determined by the Processor.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
5. 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 and the purpose of the Processing;
b. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
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.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

a. Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*) and shall not Process the Personal Data for any other purpose, unless the Processor is required to do otherwise by Law. If it is so

required the Processor shall 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, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protection Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take 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 the Contract (and in particular Annex 1 *(Processing Personal Data*));
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 Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

B. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

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 the Contract; and

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

d. not transfer, Process, or otherwise make available for Processing, Personal Data outside of the UK unless the prior written consent of the Controller has been obtained (such consent may be withheld or subject to such conditions as the Customer considers fit at the Customer's absolute discretion) and the following conditions are fulfilled:

i. the destination country has been recognised as adequate by the UK Government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;
ii. Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;
iii. the Data Subject has enforceable rights and effective legal remedies;
iv. 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

v. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

if any of the mechanisms relied on under paragraph 6(d) in respect of any transfers of Personal Data by the Processor at any time ceases to be valid, the Processor shall, if possible, implement an alternative mechanism to ensure compliance with the Data Protection Legislation. If no alternative mechanism is available, the Controller and the Processor shall work together in good faith to determine the appropriate measures to be taken, taking into account any relevant guidance and accepted good industry practice. The Controller reserves the right to require the Processor to cease any affected transfers if no alternative mechanism to ensure compliance with Data Protection Legislation is reasonably available; and

e. at the written direction, and absolute discretion, 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.

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to Processing Personal Data under or in connection with the Contract 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 the 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 Data Loss Event.

8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

9. 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 paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

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

b. such assistance as is requested by the Controller to enable the Controller to comply with a Data Subject Access 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; and/or

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.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. 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 UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

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

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

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

a. notify the Controller in writing of the intended Subprocessor and Processing that will be undertaken by the Subprocessor;

b. obtain the written consent of the Controller (such consent may be withheld or subject to such conditions as the Controller considers fit at the Controller's absolute discretion);

c. enter into a written legally binding agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor, prior to any Personal Data being transferred to or accessed by the Subprocessor; and

d. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. Any Processing by a Subprocessor or transfer of Personal Data to a Subprocessor permitted by the Controller shall not relieve the Processor from any of its liabilities, responsibilities and obligations to the Controller under this Joint Schedule 11, and the Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 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 the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure

that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data - NOT USED

Independent Controllers of Personal Data – NOT USED

Annex 1 - Processing Personal Data (Lot 1-7 Authority & Supplier, Call-Off Contract)

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1. The contact details of the Relevant Authority's Data Protection Officer are: [redacted]
2. The contact details of the Supplier's Data Protection Officer are: [redacted]
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 Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is the Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: • ***None*** **The Parties are Joint Controllers** – N/A CQC is the sole controller of the data analysed in MAXQDA.
Subject matter of the Processing	The processing is needed in order to ensure that the Processor can effectively maintain and deliver its obligations under the Framework Contract. MAXQDA is required to support Business Critical and Business BAU within the Data and Insight Unit. Data analysed in the software is routinely used to inform inspector briefings, internal staff surveys, independent voice reports. Data includes GFOC, PIR reports, Patient survey free text data, etc
Duration of the Processing	Up to 7 years after the expiry or termination of the Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder.
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this Framework Contract including; 1. Ensuring effective communication between the Supplier and CSS. Maintaining full and accurate records of every Call-Off Contract arising under the Framework Contract in accordance with Core Terms Clause 6 (Record Keeping and Reporting).

	The supplier should be responsible for first notifying CQC and then processing any periodic updates to the software as and when they are required during the contract period. The software which we will replace is MAXQDA 24 is currently used frequently by qualitative analysts in the Unit, and has been used for 5+ years. Prior to being analysed within MAXQDA, the source data will have it's own accompanying DPIA form completed and signed off. During the analysis phase, the data will be stored in a MAXQDA file-format (similar to an excel file-format), in a restricted folder on CQC's SharePoint. Data is not stored or shared with the supplier or distributor of the software
Type of Personal Data being Processed	Includes: 1. Names, email addresses, telephone numbers and communications with, CSS staff concerned with management of the Framework Contract. 2. Names, email addresses, telephone numbers and communications with, Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract. 3. Names, email addresses, telephone numbers, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract. Names, email addresses, telephone numbers and communications with Supplier staff concerned with management of the Framework Contract. Personal data my be needed in qualitative analytical projects done as part of Data and Insight workload, to support CQC's regulatory and independent voice work. This data may be used by MAXQDA in the future, for example the Patient Survey free-text data. All projects that use personal data and use this software will have an appropriate DPIA form completed before the project commences. All data used by the software will either a) not contain personal identifiably information or b) have an appropriate DPIA form

	completed when the data is collected (eg NHS Rating and Reviews, or Patient Survey free-text).
Categories of Data Subject	Includes: 1. CSS staff concerned with management of the Framework Contract. 2. Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract. 3. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract. Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Contract. The software is used to support the analysis of a range of qualitative data including; Complaints and Whistleblowing data (eg detail of complaints), Give Feedback on Care Comments (received through the webform), NHS Rate and Review comments (collected through an API) or Patient Survey free-text data (collected as part of the National Patient Survey Programme). This is known as source data. Depending on the analysis, this may or may not contain personal data.
International transfers and legal gateway	1. The Supplier shall provide CCS with a statement of the physical location where data will be stored, processed and managed. 2. The Supplier will not transfer any Personal Data outside of the European Economic Area (EEA) without the prior written consent of the Authority.
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	All relevant data to be deleted 7 years after the expiry or termination of this Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder.

Annex 1 - Processing Personal Data (Lot 8 only Authority & Supplier, Call-Off Contract) – NOT USED

Annex 1 - Processing Personal Data (CCS & Supplier, Framework Contract)

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is the Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: 1. Any Personal Data for effective communication between the Authority and the Supplier. 2. Any Personal Data for maintaining full and accurate records of the Framework Contract.
Subject matter of the Processing	The processing is needed in order to ensure that the Processor can effectively maintain and deliver its obligations under the Framework Contract.
Duration of the Processing	Up to 7 years after the expiry or termination of the Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder.
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this Framework Contract including; 2. Ensuring effective communication between the Supplier and CSS. 2. Maintaining full and accurate records of every Call-Off Contract arising under the Framework Contract in accordance with Core Terms Clause 6 (Record Keeping and Reporting).
Type of Personal Data being Processed	Includes: 2. Names, email addresses, telephone numbers and communications with, CSS staff concerned with management of the Framework Contract. 3. Names, email addresses, telephone numbers and communications with, Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract. 4. Names, email addresses, telephone numbers, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract. 4. Names, email addresses, telephone numbers and communications with Supplier staff concerned with management of the Framework Contract.

Categories of Data Subject	Includes: 2. CSS staff concerned with management of the Framework Contract. 3. Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract. 4. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract. 4. Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Contract.
International transfers and legal gateway	2. The Supplier shall provide CCS with a statement of the physical location where data will be stored, processed and managed. 3. The Supplier will not transfer any Personal Data outside of the European Economic Area (EEA) without the prior written consent of the Authority.
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	All relevant data to be deleted 7 years after the expiry or termination of this Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder.

Annex 2 – Security

The technical security requirements set out below provide an indication of the types of security measures that might be considered, in order to protect Personal Data. More, or less, measures may be appropriate depending on the subject matter of the contract, but the overall approach must be proportionate. The technical requirements must also be compliant with legislative and regulatory obligations for content and data, such as UK GDPR. The example technical security requirements set out here are intended to supplement, not replace, security schedules that will detail the total contractual security obligations and requirements that the Processor (i.e. a supplier) will be held to account to deliver under contract. Processors are also required to ensure sufficient 'flow-down' of legislative and regulatory obligations to any third party Sub-processors.

External Certifications e.g. Buyers should ensure that Suppliers hold at least Cyber
Essentials certification and ISO 27001:2013 certification if proportionate to the service being procured.

Risk Assessment e.g. Supplier should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

Security Classification of Information e.g. If the provision of the Services requires the Supplier to Process Authority/Buyer Data which is classified as OFFICIAL,OFFICIAL-SENSITIVE or Personal Data, the Supplier shall implement such additional measures as agreed with the Authority/Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

End User Devices e.g.

- The Supplier shall ensure that any Authority/Buyer Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority/Buyer except where the Authority/Buyer has given its prior written consent to an alternative arrangement.
- The Supplier shall ensure that any device which is used to Process Authority/Buyer Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

Testing e.g. The Supplier shall at their own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Authority/Buyer data being transferred into their systems. The ITHC scope must be agreed with the Authority/Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority/Buyer data.

Networking e.g. The Supplier shall ensure that any Authority/Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile

networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

Personnel Security e.g. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and,
verification of the individual's employment history; verification of the individual's criminal record. The Supplier maybe required to implement additional security vetting for some roles.

Identity, Authentication and Access Control e.g. The Supplier must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The Supplier must retain records of access to the physical sites and to the service.

Data Destruction/Deletion e.g. The Supplier must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority/Buyer data has been stored and processed on.

Audit and Protective Monitoring e.g. The Supplier shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority/Buyer Data. The retention periods for audit records and event logs must be agreed with the Authority/Buyer and documented.

Location of Authority/Buyer Data e.g. The Supplier shall not, and shall procure that none of its Sub-contractors, process Authority/Buyer Data outside the EEA without the prior written consent of the Authority/Buyer and the Supplier shall not change where it or any of its Sub-contractors process Authority/Buyer Data without the Authority/Buyer's prior written consent which may be subject to conditions.

Vulnerabilities and Corrective Action e.g. Suppliers shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

Suppliers must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.

Secure Architecture e.g. Suppliers should design the service in accordance with:

- NCSC "Security Design Principles for Digital Services"
- NCSC "Bulk Data Principles"

- NSCS "Cloud Security Principles"