Crown Commercial Service

G-Cloud 9 Call-Off Contract

This Call-Off Contract for the G-Cloud 9 Framework Agreement (RM1557ix) includes:

Part A - Order Form

Draft subject to successful quotation exercise being completed
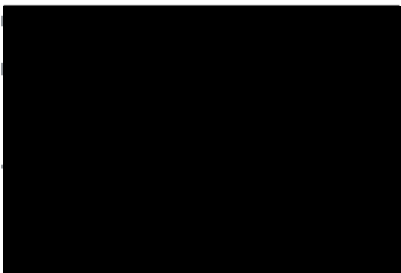
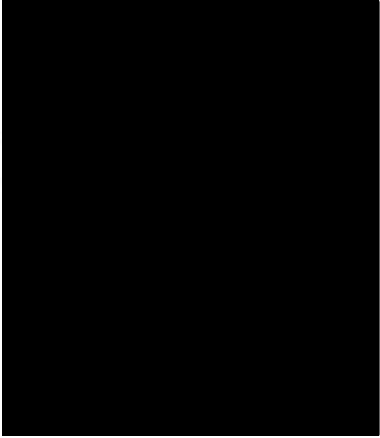|	
Digital Marketplace service ID number:	129871755243484
Call-Off Contract reference:	CQC ICTC 737
Call-Off Contract title:	Emailing Marketing System
Call-Off Contract description:	Provision to use the email marketing system used to reach external stakeholders and to communicate regular organisational messages to CQC's 3,000 staff.
Start date:	30th March 2018
Expiry date:	29th March 2020
Call-Off Contract value:	£81,072.00 (basic licence £40,536 .00 p.a.)
Charging method:	Monthly
Purchase order number:	To be provided following contract signature

This Order Form is issued under the G-Cloud 9 Framework Agreement (RM1557ix).

Buyers can use this order form to specify their G-Cloud service requirements when placing an Order.
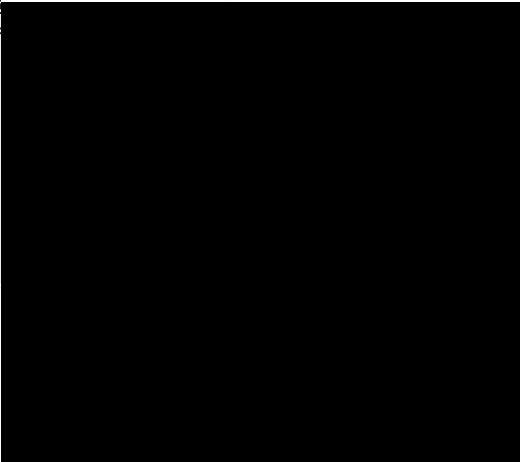
The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From: the Buyer	

	██████████
To: the Supplier	GovDelivery, LLC d/b/a Granicus ████████████████████
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title: Public Information Manager ████████████████
For the Supplier:	Title: Managing Director GovDelivery, LLC d/b/a Granicus ████████████████████

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 30th March 2018 and is valid for twenty four months
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 30 days Working Days from the date of written notice for disputed sums or at least 30 days from the date of written notice for Ending without cause.
Extension period:	N/A

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 2: Cloud Software (SaaS) GCloud 9
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:
Additional services:	None
Location:	The Services will be delivered to The Care Quality Commission 151 Buckingham Palace Road London SW1W 9SZ
Quality standards:	The quality standards required for this Call-Off Contract

Legal compliance - Compliance to all relevant nations' Legal requirements including Data Protection Act (1998) Freedom of Information Act (2001) & Privacy laws.

Data purging/archiving - There should be an option/routine to purge/archive data in accordance with an agreed data retention policy.

Support

1. Service desk & service manager - Supplier shall provide a Service Desk with ability to log and resolve incidents and requests. Supplier shall provide a named contact for escalation of issues and regular interface between the supplier and |

	the customer. **Accessibility** Accessibility – The system shall enable accessibility via assistive technology for those who cannot use a standard mouse and/or keyboard e.g. WA3, Dragon Speak and Windows 7 Voice Recognition software.
Technical standards:	The technical standards required for this Call-Off Contract are If on cloud it must be capable of hosting to ISO27001. System must also be demonstrably capable of data security standards up to and including IL2 data
KPIs and Milestones :	The service level and availability criteria required for this Call-Off Contract are referenced in Schedule 1 Section 10.
Onboarding:	The supplier currently provides this service there will be no need for on boarding this service.
Offboarding:	The offboarding plan for this Call-Off Contract is the supplier will provide a handover to agreed deliverables. Schedule 1 Section 8
Collaboration agreement:	Not Relevant
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed 125% of the contract value. The annual total liability for Buyer Data defaults will not exceed 100,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other defaults will not exceed the greater of 100,000 or 125% text of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Insurance:	The insurance(s) required will be: - a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract] - professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)]

	● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. The supplier will maintain full and accurate records and accounts, using Good Industry Practice and generally accepted accounting principles, of the: The Operation of the Framework Agreement and the Call-Off Contracts entered into with the Buyers Service provided under any Call-Off Contracts (including any subcontracts) Amounts paid by the Buyer under the Call-Off Contracts
Buyer's responsibilities:	The Buyer is responsible for N/A
Buyer's equipment:	The Buyer's equipment to be used with this Call-Off Contract includes N/A

Supplier's information

Subcontractors or partners:	N/A

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method:	The payment method for this Call-Off Contract is BACS following receipt of a valid invoice.
Payment profile:	The payment profile for this Call-Off Contract is monthly
Invoice details:	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent to Care Quality Commission , T70 Payable F175 , Phoenix House, Topcliffe Lane, Wakefield, West Yorkshire WF3 1WE
Invoice information required – for example	All invoices must include CQC Purchase Order Number to be provided at later date and Reference CQC ICTC 737

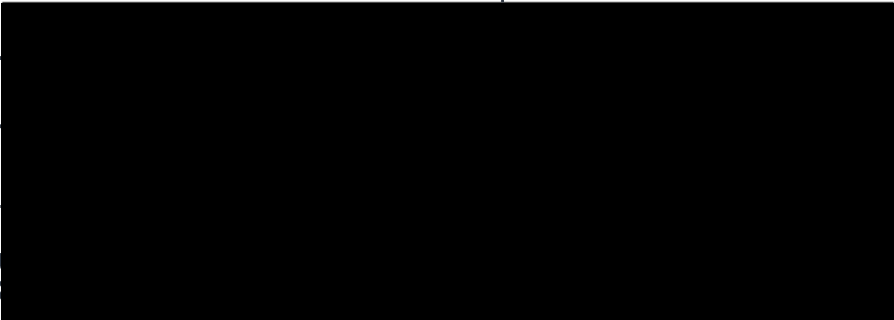|	
purchase order, project reference:	
Invoice frequency:	Invoice will be sent to the Buyer Monthly
Call-Off Contract value:	The total value of this Call-Off Contract is £67,560 + vat / £81,072 incl.vat
Call-Off Contract charges:	The breakdown of the Charges is a monthly fee of £3,378.00 incl. vat for a 24 month period.

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following key performance indicators

Indicator	Measured by	Reference Point or Target	Review Date
Any system is required to meet service availability levels of 99.5% Monday to Friday. 5 days a week with the exception of UK bank holidays	The GovDelivery Communications Cloud service availability is routinely measured by the Uptime Institute (external company)	Granicus will strive to maintain uptime availability levels of 99.9%, however will notify CQC if levels drop below 99.5%	Reviewed 2-weekly
System Maintenance outside working hours	GovDelivery Technical Operations	Granicus will strive to provide system maintenance and releases outside normal business hours as much as possible. The 99.9% service availability figure includes planned system maintenance.	Reviewed 2-weekly

Guarantee:	N/A
Warranties, representations:	N/A
Supplemental requirements in addition to the Call-Off terms:	N/A
Alternative clauses:	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms:	N/A
Public Services Network (PSN):	The Public Services Network (PSN) is the Government's secure network. If the G-Cloud Services are to be delivered over PSN this should be detailed here: N/A

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557ix.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name:		
Title:		
Signature:		
Date:		

Schedule 1 – Services

CareQuality Commission

Commission

CQC reference CQC ICTC 737

Emailing Marketing System

STATEMENT OF REQUIREMENTS

Technical Response

Name of Tenderers: GovDelivery, LLC d/b/a Granicus

Contents

1. Executive Summary

Since January 2016, the Care Quality Commission (CQC) and Granicus have been working in partnership delivering a market leading digital communications service – the GovDelivery Communications Cloud - which has proved successful in allowing CQC to rapidly grow its audience and engage with them, delivering granular, highly targeted information, to the public, its stakeholders and internal staff. This relationship has been so successful that the number of external subscribers receiving messages from CQC has grown to 154,000 with 389,000 subscriptions - resulting in the sending of 3,200,000 messages in the last 12 months. These figures are taken from the reporting tool that CQC has full access to via the portal.
The unique enabler for achieving this, is having access to the GovDelivery collaboration network which currently comprises of over 11 million UK citizens. The impact of this Network over the last two years at CQC has been huge. By collaborating with Public Health England, Food Standards Agency and the HSE, along with many other central and local government organisations, CQC has been able to attract, and engage with more people than through traditional means. There has been a 95% growth in new subscribers as a direct result of the GovDelivery Network.

In addition, CQC uses the Communications Cloud to inform its 3,300-internal staff, sending 50,000 messages with an engagement rate of over 90% over the last year. The combination of internal and external messaging has created 3,250,000 messages in the last year; all of which is covered by the fixed monthly charge with no hidden / increased charges or volume limitations. There is no penalty to CQC's success.

This growth in reach and messages sent, has enabled CQC to raise and increase awareness of its services with a larger cross-section of stakeholders. The take up of individual subscriptions and the engagement levels of specific emails has helped to inform CQC strategy.

From listening to and understanding the public's desire for specific information, CQC is able to invest in creating high quality, focused messages which inform and educate the public, helping them to make better decisions about care, thus improving a wide range of outcomes and ultimately improving the quality of life of the general public.

In the ITT documentation, it is clear that CQC want to build on the success it has previously enjoyed, whilst continuing to accrue the current benefits of a Software as a Service (SaaS) cloud delivery. This type of delivery does not put any increased overhead on the CQC IT team or current network/infrastructure and is the service delivery route for Communications Cloud - all the equipment and support is supplied by Granicus via "The Cloud" with no hardware or software for CQC to install and administer.

The GovDelivery Communications Cloud has been designed purely for the Public Sector with key objectives in mind such as, ease of use by authors / administrators who are specialists in their areas of expertise without the need for the communications team to be constantly involved.

As you would expect from the market leading solution, a variety of support tools from online FAQs and a comprehensive support portal, to a freephone 24 x 7 support line are all available to assist our customers

with any application queries. In addition to this, an Account Manager is assigned to all customer accounts along with support from a Success Consultant to work closely with CQC to understand the Communications Strategy and to support the team, ensuring usage is aligned to, and that the service is used in the best way possible to help achieve CQC's strategic objectives.

To improve and enhance the service, CQC are looking at ways to be able to automatically segment their audience into discreet stakeholder/interest groups, with the aim of being able to engage an "opt-in" audience on granular topics with greater audience segmentation. In addition, it is CQC's desire to be able to contact dormant subscribers and re-engage with them and A/B test messages. The Granicus solution offered in this response will add these desired enhancements to the already highly successful GovDelivery Communications Cloud solution that is in place.

By taking the step to improve and extend the current scope to the Professional license, the features described above should directly have an even greater impact in CQC's engagement efforts by getting the right information, to the right people, at the right time; resulting in better lives for more people -- something we at Granicus are passionate about and is deep rooted into our ethos of helping government be better and changing lives. Automation, better segmentation of subscribers, and message testing capabilities within the extended license will help CQC get faster results, with less time and effort.

Adding the "desirables" to the current system could not be simpler for CQC as it requires no more input or equipment other than a purchase order. Granicus would then upgrade the license, grant access to these additional features, in addition to providing sufficient training and a hands-on consultant who will guide CQC through every aspect of the tool to ensure long-term success. The pricing for this is clearly broken down in the Commercial response.

In activating the desirable features, CQC would be upgrading their current basic license to the GovDelivery Communications Cloud "Professional" service, and joining the rapidly growing number of customers who are currently using the service to better reach and engage with their audiences.

Activating these features will increase CQC's current fee by £1093 + vat p/m, with the total monthly fee being fixed for 24 months as per the current G-Cloud (9) framework agreement with no hidden / increased charges, and free from any sending volume restrictions. There is no penalty to CQC's success. In addition, there would be a small (one-time) set up fee of £4,056 + vat to cover the additional training and license upgrade work required to the current live service.

With digital communications, and specifically email marketing, getting more and more advanced, using the GovDelivery Professional Communications Cloud service, CQC can expect to take its communications to the next level. Testing messages to ensure the best possible version is going out using sophisticated and automated capabilities, combined with targeting the right people and segmenting audiences, is a proven way of getting the right message to the right people to drive better actions and outcomes.

These campaigns, as described above, would allow CQC to better engage with subscribers from day one, build better relations, and ultimately increase the impact the messages are having. Taking advantage of these high-impact e-marketing features which are used extensively across the private sector, and gaining rapid traction within the public sector, will allow CQC to achieve more tangible results from their communications efforts without relying on large teams to administer, analyse and refine on a regular basis, thanks to the automation and reporting capabilities within the platform.

We strongly commend the GovDelivery Communications Cloud complaint solution to CQC. Being a live service, already implemented, and with multiple trained administrators using the platform, it is a very low risk option for the business. There would be no service down-time or any effort internally at CQC required for continued usage beyond the upcoming renewal date.

Communication Cloud - Service Overview

Thought leaders have moved beyond basic outbound email newsletters and simple email alerts. GovDelivery Communications Cloud offers significantly more than traditional systems by focusing on rapid subscriber growth combined with the ability to deliver highly targeted, multi-media dialog between government and stakeholders.

GovDelivery Communications Cloud has been developed specifically for the public sector and operates within a secure Software-as-a-Service (SAAS) platform. Our digital subscription management solution enables clients to utilise marketing automation, advanced electronic newsletters and the ability to provide highly granular updates to the content they publish online.

GovDelivery Communication Cloud delivers notifications and alerts using the most important digital channels including email, SMS, RSS and Social Media tied directly to website updates and publishing of new information. By offering proactive public communications, CQC can quickly, efficiently and effectively reach a large number of highly engaged stakeholders whenever necessary.

CQC already benefits from the extensive experience we have gained by working in partnership with leading public sector organisations to significantly grow their online audience and digital subscribers.

At the heart of the Communications Cloud service is a unique collaboration network which enables CQC to cross-promote subscriptions with other government organisations to reach more people and grow the audience base. Cross-promotion enables CQC to collectively benefit from surges in visitors to a particular website. The overall result of this inter-government collaboration is a more informed nation, with citizens making better decisions.

For example, nearly 1 in 9 subscribers to National Audit Office alerts have signed up through another government agency via the GovDelivery Network. These are subscribers who haven't visited the NAO website. CQC has already built as impressive subscriber lists with the help of this cross-promotion capability. Another example is the Met Office who have over 257,000 subscribers of which almost 50% have come through our network.

As a result of the Communication Cloud Network and our focus on maximising subscriptions, the single biggest benefit for public sector organisations like CQC when using the GovDelivery Communication Cloud solution is the ability to reach, engage and convert the largest possible number of citizens and stakeholders to action.

REACH — The services you deliver are only as effective as your reach.

ENGAGE — Providing the right information to the right audience, at the right time, is critical.

CONVERT — Targeted messaging driven by audience behavior gets results.
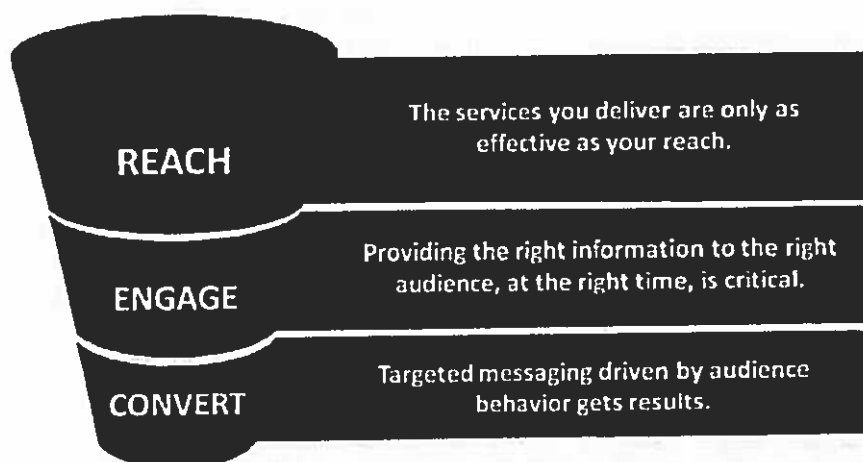
Figure: More actively engaged citizen's results in better engagement, greater awareness and drives more effective outcomes.

Results from our many clients indicate you will build a large subscriber base using the GovDelivery Communications Cloud platform (local authorities report reaching 20-30% of their target population). Clients can expect to reach, engage and inform hundreds of thousands of citizens across the UK who would otherwise be difficult to reach.

Central Government	Audience Size
CQC	155,000
MHRA	134,000
MRC	35,000
Public Health England	185,000
Department for Work and Pensions	99,000
Department for Business, Energy and Industrial strategy	90,000
Driver and Vehicle Standards Agency	351,000
Driving and Vehicle Licencing Agency	181,000
Parliament	196,000
Government Digital Service (used on GOV.UK)	733,000
Her Majesty's Revenue and Customs	4,100,000
Highways England	205,000
Met Office	257,000
Ministry of Justice	125,000
National Audit Office	35,000
Office for National Statistics	78,000
UK Space Agency	74,000
Welsh Assembly Government	238,000
Health and Safety Executive	521,000

Figure: Communications Cloud is helping government reach and engage large numbers of people.

Communications Cloud – Top Ten Benefits

The benefits of implementing the GovDelivery Communications Cloud solution extend much further than the ability to send newsletters and alerts to a small numbers of subscribers. Our ability to reach the largest possible audience with accurate, timely information delivers the biggest benefits to both subscribers and public sector organisations.

1. **Reach more stakeholders with timely communication.** Build a large base of stakeholders by offering highly personalised opt-in subscription options. More choice helps CQC generate over **100%** more subscribers than using traditional email newsletter, alerting or social media software.

2. **Increase Website usage.** Increases visits and return visits to CQC websites and social media channels such as Blogs, Facebook, Twitter and YouTube. More traffic means many more online transactions will be completed with typical clients seeing a **35%+** increase in visitors. Clients with best practice implementations like CQC should find that GovDelivery will be in their top 5 referrers of all traffic to their website.

3. **Improve audience satisfaction.** Proactive communication through Communications Cloud has been shown to increase stakeholder satisfaction and perception of websites and associated online services.

4. **Reduce administrative headache.** Message alerts are integrated with websites to automatically send alerts when RSS, website content or other online channels (YouTube, Twitter, Blogs, Flickr, etc.) change. GovDelivery streamlines the administrative process of sending messages and managing subscribers, eliminating the time and risk of separately managing and approving notices to stakeholders.

5. **Measurable effectiveness of communications.** All messages can be tracked and audited to see when opened and read. Click-throughs can be monitored to see which users clicked on which links to verify the value and success of your communications. Further management reporting is available via the GovDelivery User Portal, providing analytics for Account Performance, Bulletins, Subscribers, Subscriptions, Topics, etc.

6. **Create a single view of the Subscriber.** GovDelivery generates detailed demographic information that shows what services individual users are interested in, their location, age group etc. All messages are tracked and audited to show click-through, as well as engagement rates, enabling detailed targeting of messages to specific user groups.

7. **Customised, single point of service for subscribers.** Allow Subscribers to create a comprehensive profile of information they wish to receive from Government. Subscribers can also sign-up for email, personalised RSS feeds, Twitter/Facebook and SMS text alerts depending on the information requested.

8. **Hosted (Software-as-a-Service) solution.** Fast setup and fully scalable platform requires no hardware or software and does not impact bandwidth. Full support and management of email delivery and bounces is included.

9. **Technology Agnostic.** GovDelivery integrates with any CRM or CMS system – an option available to CQC should they wish to have explore.

10. **Secure.** Security is a paramount concern to clients; therefore, it is a top priority for GovDelivery. Communications Cloud operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013, meets G-Cloud assurance requirements and is Privacy Shield compliant.

Communications Cloud – Feature Overview

The GovDelivery Communications Cloud service has been developed specifically for the public sector. Communication Cloud operates as a software-as-a-service (SaaS) digital subscription management solution and enables clients to provide both newsletters and granular subscriptions to the content they publish online.

The following section provides a high level overview of the key features, benefits and use cases for users of the Communication Cloud service.
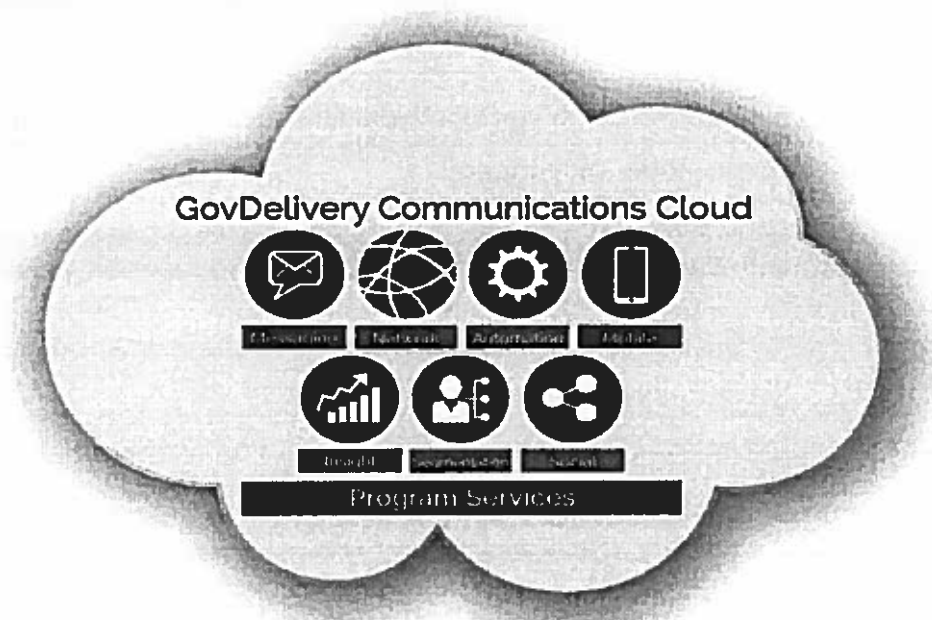

Figure: GovDelivery provides far more than basic email management. Full multi-channel communication is supported.

GovDelivery Communications Cloud

Messaging	Create and send messages that get people to take action with GovDelivery's comprehensive messaging tools. GovDelivery can handle a variety of messaging needs from the real-time automated distribution of alerts on specific topics to mass notifications during emergencies or pre-built, branded newsletter templates.
Network	Increase the number of people who you reach by 100%, 500%, or even 1,000% by cross-promoting your most important programs and events with the largest network of government communicators in the world on the GovDelivery Network.
Automation	**Achieve a return on investment (ROI) of up to 200%** in the first year with reduced printed mail and postage costs by streamlining your content distribution across email, text messages, and social media channels to conserve resources and improve organisational efficiency. Create messages once; publish them anywhere.
Mobile	Communicate with your stakeholders wherever they are by delivering optimised messages directly to mobile devices. You will reach people where they have the best chance to act with GovDelivery's full suite of mobile tools.
Social	Leverage social networks to strengthen your direct connections and amplify social content by promoting and sharing in new and more effective ways. Drive more traffic to social content by consuming content from social media and automatically promoting it to your most active audiences.
Segmentation	Target specific members of your audience for optimal engagement and messaging success. Customise subscriber questions to segment the audience and tailor messages to be more relevant and actionable.
Insight	Measure the impact of your actionable initiatives and improve communications with a robust analytics dashboard that helps your better understand what types of content resonate with the intended audiences.

Additional GovDelivery Capabilities

Targeted Messaging	
Programme Services	
Professional Package	

Improve business and digital communication processes with reliable delivery and robust tracking of any message sent from applications or systems in an organisation.

Use GovDelivery's proven team to expand outreach, build and support online communities, or encourage digital conversion (reduction of paper communications and business processes).

Use the optional Professional Package to send highly targeted and automated marketing campaigns, dynamically segment your audience based on actions and preferences, and access automated A/B testing functionality to drive greater action and engagement.

Communication Cloud – Key Features

Messaging
We enable CQC to provide granular subscriptions to the content they publish on-line and provide notifications and alerts using the most important digital channels including email, SMS, RSS and Social Media when this content is updated. Offering proactive public communications allows our clients to quickly, efficiently and effectively reach a highly engaged audience whenever necessary.
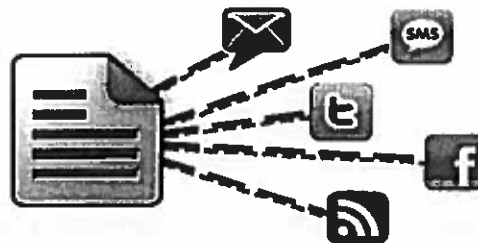
Figure: Create Once Publish Everywhere (COPE) content distribution model.

Comprehensive messaging tools allow you to create messages that get people to take action.

- Create and distribute emails, text messages and social media updates all from a single platform.
- Use pre-built and branded templates, specifically designed to drive audience engagement.
- Trigger branded and/or automated messages to your stakeholders, using updated web content, new blog posts or social media updates.
- Edit and approve communications prior to sending with permissions-based workflows.
- Reach the inbox with unparalleled industry deliverability rates.

17

| Newsletters | Automated Alerts | Mobile Alerts | Social Media Alerts | Shareable Widgets |

We help manage over 175 million individual subscribers on behalf of over 1,800 public sector clients and currently send over 12 billion messages a year for them. The service is secure, robust and highly scalable. GovDelivery invests considerable effort to ensure that our clients' messages arrive in inboxes. We achieve inbox delivery rates in excess of 99%, which is significantly above the industry average.

As we send messages exclusively for public bodies we are able to maintain strong relationships with Email Service Providers (ESP). This ensures messages sent via GovDelivery are not identified as email spam which is particularly important where important public information messages include spam filter trigger words such as "drug abuse".

Network

The unique GovDelivery Network is a key strategic tool in delivering high subscription volumes and deep engagement across UK Government. The GovDelivery network is huge. It includes nearly 11 million UK subscribers with the total international audience of 175 million subscribers.

The Network allows a subscriber to reach other government organisations because messages and alerts are cross-promoted from related agencies, e.g. subscribers to Southampton Stay Connect Alerts are being offered other clients' alerts e.g. Met Office Severe Weather Warning and newsletters to significantly boost take up of e-Services and quickly raise awareness of activities and projects.

CQC's impact has been significant over the last 12 months with subscribers engaging with CQC content from other GovDelivery users including PHE, MHRA, HSE and the Met Office to name a few.

Using geo-intelligent technology, the Network is able to make local subscription recommendations based on the subscribers' approximate location. Therefore, subscribers to Highways England could be offered Missed Bin updates if they are located in Kirklees.
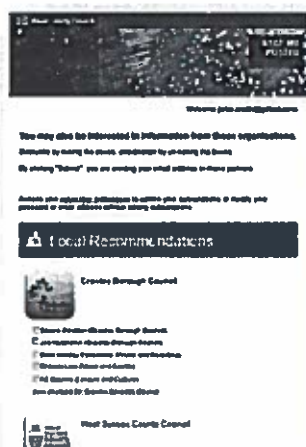

18

Figure: Promotion of local recommendations and alerts from suggested network partners can boost subscriptions by up to 500% in this example the subscriber is based in West Sussex hence local recommendations shown.

Automation

Use extremely flexible automation tools to conserve resources and improve organisational efficiency. Our innovative "PageWatch" technology monitors clients' online channels for content update and then sends messages to subscribers when certain predefined automation actions apply for each topic. Options include sending the alert automatically or to ask an administrator to approve the message. Alerts can be delivered as emails, SMS, social media posts and personalised RSS feeds.

- CQC currently enjoy the benefit of automating social media posts to subscribers, freeing up internal time and resource.
- Instantly send multichannel messages to your audience when content is updated on digital properties.
- Create messages once; publish them everywhere.
- Use templates and workflow rules to distribute messages automatically or after administrative approval.
- Benefit from a rich set of APIs to facilitate integrations and serve a variety of functions.
  Build your audience and deliver content with pre-built GovDelivery modules for Drupal, WordPress, and Facebook.

Mobile

Communicate with your stakeholders wherever they are, by delivering messages directly to their mobile devices with our Mobile module. This allows you to reach more people wherever they are to increase your chances of getting more people to take action.

- Responsively designed sign-up pages make subscribing from a mobile phone as easy as possible.
- Mobile-enabled email offers opportunities to deliver rich and actionable content to mobile devices.
- Targeted direct text messaging capabilities complement email and other channels.
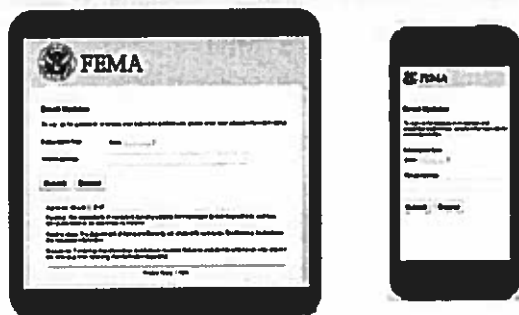- Utilise automated text messaging to deliver dynamic content to people on the go.

Figure: Responsive design ensures an easy to use sign-up process on a wide range of mobile devices.

Insight

Improve your communications by measuring the impact of your outreach and communications.

Use actionable Insight to gain valuable metrics for continuous improvement. Highlighting the metrics you need to measure your communications performance and improve outreach and engagement. When performance increases you reach more people and get those people to take action.

- Access a complete Account Performance Report with high-level metrics that show audience growth and engagement over time.

- Automatically deliver valuable metrics to key internal stakeholders and management with report-sharing functionalities.

- See all messages across CQC in one system with detailed analytics (opens, clicks, etc.) to track and demonstrate communications value.

- Utilise GovDelivery's communications and outreach experts to conduct deeper analyses that can map communications to program or mission goals for greater impact.

Key Metrics

Figure: A wide range of dashboards and reports provide detailed insight in to who, how and when your messages are being used.

Segmentation

Delivering effective content means reaching the right people with the right message. GovDelivery helps you target messages more accurately with a comprehensive segmentation module.
Target specific members of your audience for optimal engagement and messaging success.

- Offer a large number of highly-relevant subscription topics so your audience can tell you what they're
interested in.

- Customise subscriber questions, from post code to school district to homeownership status, or more, to segment your audience and tailor messages to be more relevant and actionable.

- Filter message recipients on criteria such as previous recipient activity, opens or clicks, date added, and more.

- Run A/B tests to optimise your content for maximum engagement.

Helping you focus your digital communications on the right people. And reaching the right people means driving increased stakeholder engagement.

Social

Leverage social networks to strengthen your direct connections and amplify your social content with our
Social
connectivity.

Figure: Modern communicators need to support a wide range of digital channels.

While email and text messaging are the foundation from which to build digital outreach, social media plays a powerful and complementary role. Get your digital audience to actually see and engage with your social content.

- Drive more traffic to social content by consuming content from Twitter, YouTube, Tumblr, Flickr and other networks and sending it to your most active audience.

Allow people to share messages across the most popular social media channels to expand your reach.

Cross-post content to social media when sending out information by email and text message.

Leverage social accounts by offering social sign-up options and using applications to bolster outreach tactics.

Overview of sign up process

The following overview provides a step-by-step explanation of the GovDelivery Communication Cloud service from the subscriber's perspective using the example of the service we provide to CQC Subscribers

Subscriptions can be provided from anywhere on the client's website or social media pages. Simple "HTML "Snippets" are provided during implementations that are used to link your website to the subscription service.

21

Figure: Highly visible sign up links ensure maximum engagement with website visitors

Sign-up

The subscriber provides their email address/SMS number or can opt to sign in using a social media account. You can allow subscribers to decide how often they hear from you. Subscribers can add a password to their profile if they wish to.

Figure: All subscription pages can be fully branded to contain agency logos and brand. Sign-up process is designed to be clear and simple to maximise subscriptions.

Granular Opt-in

The subscriber selects topics that they would like to subscribe to by checking the boxes. This approach is a great way to cross-promote other service areas and ensure a single interaction with a subscriber is magnified to all the areas that are of interest to them. There is no limit to the number of topics that can be provided which enables clients to offer alerts that are highly targeted to each individual subscriber's interests.

Collect data about subscribers to tailor the communications they receive

Ask Questions (Optional)
The subscriber is invited to provide further information about themselves based upon the subscription topics they've selected. This helps CQC to get to know their audience and tailor messages far more accurately.
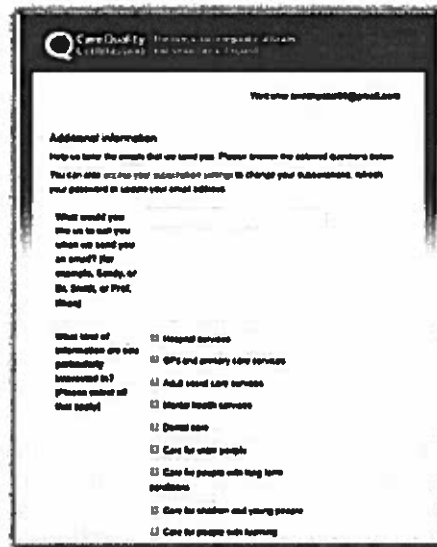
Figure: Ask questions to generate detailed demographic information to gain more valuable insight into subscribers.

Leadership

CQC seeks to establish that the chose supplier has the appropriate leadership, expertise and credibility in the field, and the skills, qualifications and experience to lead the scope of the service delivery requirements.

CQC require the supplier's leadership arrangements to be sufficient and suitable to ensure successful delivery, with a resource team involved in the implementation being suitably experienced and qualified.

Offices

Granicus has offices in in St. Paul, Minnesota, Washington, D.C., Denver and Gatwick, United Kingdom. The Granicus team thrives on helping government organisations improve communication and engagement with the public. Our leaders are passionate about developing innovative technologies and working side-by-side with government.

Leadership

██████████████████████████████ currently serves as CEO of Granicus. Prior to Granicus and since 2010, Mark served as Chief Strategy and Development Officer as well as President, Technology Services, for Altisource, a public real estate and mortgage technology and services company. Before joining

23

Altisource, he served as President of Digi-Net Technologies, Inc., an early pioneer in marketing analytics software-as-a-service solutions.

███████████ **Chief Product Officer,** has more than 30 years of experience in technology and software development, fulfilling senior positions ranging from software engineering, to sales and marketing, to strategy and chief executive officer.

████████ **CFO.** As the Granicus Chief Financial Officer, ███ is a client-focused executive with a proven track record leading and managing change and impacting business results by leveraging a broad experiential base of strategic planning, financing, acquisitions, financial management, and process improvement. Prior to coming to Granicus, Eric served as an Executive Vice President and CFO for Dimension Data.

████████████ **EVP of Sales,** ████████ oined Granicus in 2015, leading the teams that grow the company's client base and expanding work with existing clients. With his extensive range of experience, from technology start-ups to major firms serving the public sector, ████████ rings invaluable growth experience and government expertise to the Granicus team.

████████ **Managing Director GovDelivery Europe,** has over 15 years of experience consulting on and developing advanced information management, electronic publishing and communication systems. Having previously worked for The Stationery Office (TSO), ████ is well versed in the challenges that public sector organisations must overcome in order to deliver timely, accurate and relevant information to the public.

████████████ **VP of Product Management,** Laurel leads the Product Management team, which is focused on bringing software to market that helps the public sector connect with citizens. Laurel has held a variety of product roles at ING DIRECT / Capital One 360, the largest online bank in the U.S. ████ olds an MBA from the Kellogg School of Management at Northwestern University.

████████ **Director of Implementation,** Cindy and her team enable clients (new and old) to drive measurable success with their GovDelivery Communications Cloud integrations. With over a decade of Project Management experience in digital communications, ████ inds great joy in the program success that makes it all worthwhile. Cindy has a BA from the University of Wisconsin – River Falls.

Granicus Staff

There are approximately 350 staff employed by Granicus across the US and Europe. While a number of staff have access to the service the key roles for the fulfilment of this service, from the UK office staff are as follows:

███
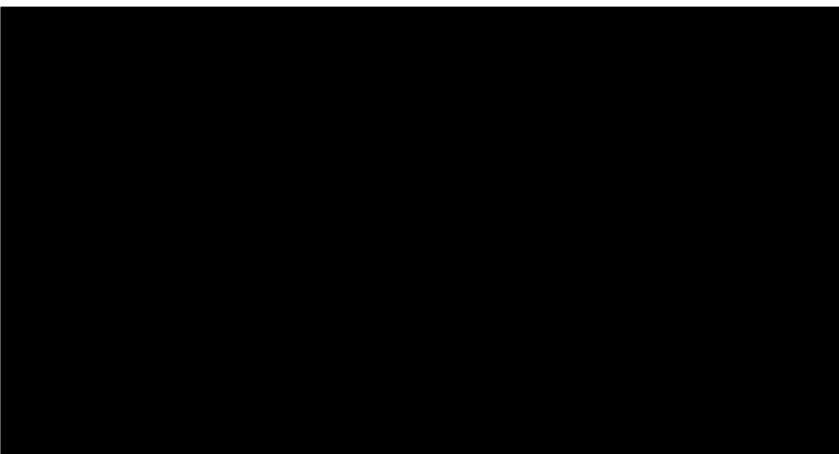
A number of support staff based in our US office have access to the Communications Cloud system and report directly to the senior staff identified below.

█████████████ leads a large team of dedicated support professionals who are on hand 24/7 to help all our customers with any issue or request concerning the service. CQC would continue to have access to this customer support service as a core part of the licence and would include email, Freephone telephone and live online chat support.

CQC seeks to establish that the chosen supplier has the appropriate leadership, expertise and credibility in the field, and the skills, qualifications and experience to lead the scope of the service delivery requirements.

CQC require the supplier's leadership arrangements to be sufficient and suitable to ensure successful delivery, with a resource team involved in the implementation being suitably experienced and qualified.

As outlined above, Granicus has demonstrated that it has a highly skilled and experienced leadership team along with a first-rate implementation team to continue delivering the existing service CQC have, along with any additional implementation activities that may be required.

The Implementation team consists of a wide range of personnel including Project Managers, Consultants, Technical Consultants and Trainers – all focused on helping our customers get up and running with the service, and providing on going and continual support should the need arise.

Method Statement

Granicus has clearly demonstrated in its response and current service provision its full compliance with the requirement of this procurement.

Given the service is live and as mentioned above, no implementation activities would be required for continuation of the existing basic licence; continuing with the Communications Cloud service would a low-risk, low cost option for CQC. The service has delivered impressive results over the last 2 years and we are keen to help CQC make even greater use of the platform.

Should CQC opt for the Professional Licence, which is detailed in later sections of this response, a small amount of setup and configuration along with dedicated administrator training would be provided by an experienced Implementation Consultant to ensure the organisation gets the most value from the service.

Has a credible solution

As demonstrated in this response, the GovDelivery Communications Cloud service is a highly credible and trusted platform built for, and used exclusively by the public sector. The platform is focused on delivering highly targeted, granular digital communications to audiences using the latest and most cost effective digital channels.

The service has been used successfully by CQC for the past two years, joining 1,000's of other public sector organisations globally. We are excited to work more closely with the CQC team going forward to take communications to the next level, with a focus on more segmentation to better target groups of subscribers, refining messages to drive the most action. Making use of automated on-boarding and re-engagement campaigns to create more value with subscribers, further increasing action and outcomes which make a difference to subscribers and CQC.

Granicus has a dedicated team of individuals all suitably experienced to deliver a first-class service. The implementation team have many years of experience in delivering the GovDelivery solution to over 1,800 government organisations globally. If the licence is upgraded, a dedicated, named contact will be assigned

to the project and this individual will liaise with personnel at CQC to be on hand at every step of the implementation.

Has a defined and achievable timeline

As mentioned above, with the service being live, no implementation activities would be required for continuation of the existing basic licence (business as usual), however a small amount of setup and configuration along with dedicated administrator training would be provided by an experienced Implementation Consultant, should CQC opt for the Professional Licence.

Granicus is able to activate the Professional Licence instantly upon agreement to proceed. An Implementation Consultant would be assigned within one week of the contract start to administer training and any configuration or build activities needed.

The current Account Manager would liaise with the current CQC contact to arrange these activities.

Section 12. "Milestones" outlines the activities required for a licence upgrade and the associated timescales.
Has identified and proposes suitable management of the delivery risks

The previous section "Leadership" outlines the extensive, highly experienced management within Granicus who are well versed in delivering similar services and implementations on a daily basis.

Granicus has no concerns delivering this solution to CQC and has more than adequate resource to ensure success.

Given the current service is due to expire on the 29th January 2018, continuing to use the GovDelivery service which is live, fully configured, and requires no additional effort or implementation by us or CQC, makes GovDelivery a low-risk and viable solution.

CQC and its large subscriber base would not experience any service downtime and there would be no adverse business impact, should CQC continue with the existing Communications Cloud service.

Has a quality assurance regime that monitors, measures and assures quality outcomes

Right from an initial project kick-off meeting for new customers, to the end of a contract and off-boarding from the service, Granicus staff ensure that every step and interaction with us, is a successful one.

The Implementation team, who would be involved in any upgrade to the Professional Licence, would work with CQC staff and make sure that CQC are fully satisfied with the service and are comfortable using all features within the account, prior to handing off to the dedicated Account Manager.

The role of the Account Manager or Success Consultant would be to work closely with CQC to use the platform in the best way possible to drive outcomes and success.

Gone are the days of SOS (sending out stuff) communications; messages need to be clear and outcome focused – driving real and measurable impact. Identifying high impact areas/business requirements and mapping this to usage is something that we love to get involved with and this would be the role of the Success Consultant to work with the CQC team on.

The current GovDelivery Communication Cloud configuration was previously assessed by the UK Government Communications-Electronics Security Group (CESG) and was previously accredited to UK Government Impact Level 2 (IL2) – Secure. GovDelivery holds ISO27001:2013 certification which identifies strict procedures for managing, monitoring and mitigating risk. We follow these procedures rigorously as part of our on-going ISO27001 and other security accreditations.

In addition to the above accreditations, GovDelivery is registered with the Information Commissioners Office (ICO) and the European Union Privacy Shield programme for management of data. GovDelivery security

policies and procedures are also in accordance with US National Institute of Standards and Technology ("NIST") standards.

The service undergoes an annual certification and accreditation audit by NIST. GovDelivery is also one of a few select organisations approved by the Federal Risk and Authorization Management Program (FedRAMP) US government-wide security authorisation programme.

Our highly secure environment has withstood comprehensive and rigorous review at the JAB level, approved by CIOs from the General Services Administration (GSA), the Department of Defense (DOD) and the Department of Homeland Security (DHS). NIST reviews our Security Plan, Continuity of Operations Plan and Threat and Risk Assessment as part of the certification and accreditation audit.

Being an already live service, CQC can rest assured that continuing with GovDelivery, is the lowest risk option for the organisation.

Implementation and Resource

CQC seeks to establish that the supplier has the level and quality of resources to deliver the scope of the service/delivery requirements and the timeline within which they are able to deliver each aspect of the functionality

With Communications Cloud being a live and already implemented service, CQC would not require any implementation activities in renewing the service on the current basis. CQC can assume business as usual and continue using the Communications Cloud service as it does now without any disruption, configuration or setup activities.

Should CQC opt for the recommended GovDelivery Professional Licence, there will be a dedicated Implementation Consultant (from Cindy Hoops' Implementation Team) assigned to the project. This individual would work closely with CQC staff to train, setup and fully configure the Professional package. These activities would include but not be limited to, template creation, the setup of any on boarding or re-engagement campaigns, and full training sessions for staff.

Granicus has a large team of individuals all suitably experienced to deliver a first-class service. The dedicated implementation team have many years of experience in delivering the GovDelivery solution to more than 1,800 government organisations globally. Our implementation team enable clients like CQC to drive measurable success with their GovDelivery integrations.

2. The Requirement

CQC EMAIL MARKETING SYSTEM REQUIREMENTS

Background

To meet our objectives (detailed below), sending direct communications, such as email letters and e-bulletins is vital for CQC. Email is our main method of mass direct communication.

1. We wish to use the email marketing system used to reach external stakeholders and to communicate regular organisational messages to CQC's 3,000 staff.

    Noted and Understood.

    Communications Cloud delivers over 11 billion messages for worldwide government each year. It can easily scale to cope with any increase in use and hence the figures outlined by CQC are easily accommodated. For reference, we frequently send over 200 million messages for UK government each

month. We are proven to work at scale and current meet the needs of CQC with significant spare capacity.

Granicus does not charge per email message sent. We have a flat monthly fee which is fixed throughout the annual contract irrespective of the number of emails sent.

Our fixed fee approach allows CQC to budget accurately and not be concerned with large peaks in message volumes. CQC can rest assured that as usage expands across the organisation, there will be no cost implications or restrictions to limit success.

The organisational objectives directly dependent on an effective email marketing system are as follows.

Public engagement team objectives:

2. Raise awareness and understanding of CQC's role and purpose
3. Listen to and act on the public's views and experiences of care
4. Co-produce the design and shape of our work with the public
5. Provide high quality information to help people choose care

The GovDelivery Communications Cloud service is fully compliant with these four objectives. With the GovDelivery Communications Cloud service, we effectively create a partnership with CQC, whose creatives will create high quality information and message content. GovDelivery will deliver this content reaching the right people with the right message - one size does not fit all. GovDelivery helps you target information more accurately with a comprehensive segmentation module.

Target specific members of your audience for optimal engagement and messaging success.
- *Offer a large number of highly-relevant subscription topics so your audience can tell you what they're interested in.*
- *Customise subscriber questions – CQC currently gather various data from new subscribers, including "Name", "Interests" and "Locations" – allowing you to tailor messages to be more relevant and actionable.*
- *Filter message recipients on criteria such as previous recipient activity, opens or clicks, date added, and more.*
- *Run A/B tests to optimise your content for maximum engagement.*

GovDelivery records approximate locations of subscribers to all accounts, via dynamic IP addresses, (where available). This enables segmentation based on location, this is called Geo- Smart.

An example of this use could be that if CQC wanted to engage with more people in the Liverpool area, Geo-Smart will monitor sign ups from the area on all other accounts. When the subscriber finishes their initial subscription, they would be offered the opportunity to sign up for CQC information. In this way actively reaching and engaging more people and helping CQC focus its digital communications on the right people would result in increased stakeholder engagement.

As described in other areas of this response, the GovDelivery service has a full set of analytical tools which are available via the secure portal. These tools will provide the feedback which in turn will help to inform CQC message Content.

Granicus will assign Account Managers to support clients with best practices and share better ways to improve quality with lesson learnt from other clients. Working closely with the team there, Granicus Account Managers and Success Consultants are able to meet with CQC to discuss the strategy and help shape the service and public offering to drive desired outcomes and successful outreach with the public.

It should also be borne in mind that Granicus is able to assist with the creation of compelling material and

campaigns via its professional services team. In addition our support function comprises of experienced graphic designers who are on hand to work with CQC to create engaging templates to maximise the impact of messaging. There is no additional cost associated with this service and allows CQC to free up design resources and save money.

As previously mentioned, in the past year CQC benefited from a 95% growth in new subscribers through collaboration on the Communications Cloud network. These are all subscribers who would not have naturally signed up through usage of CQC channels and therefore, can be seen as a valuable bonus to the business in engaging and raising greater awareness of CQC's role and purpose.

Other government clients have successful used this enhanced reach to gather feedback on services, and conduct surveys of their large audiences. Typical engagement rates exceed 65% for many clients.

For example, the Driver and Vehicle Safety Agency has a combined GovDelivery audience of 351k subscribers with a 65% engagement rate. CQC can effectively use the platform to promote the completion of surveys with new and existing subscribers helping to gain valuable insight from customers and help CQC listen to, and act upon the public's views and experiences of care.

In many government agencies, GovDelivery messages are being used to increase Website usage. This increase in traffic can be directly delivered via a URL to specific areas and questionnaires on your website designed to capture feedback. More traffic means many more online feedback questionnaires will be completed, with typical clients seeing a 35%+ increase in visitors to their website.

The CQC website contains lots of information from guidance, tips, and guidance and inspection reports. Having a large and engaged audience to communicate with means CQC can successfully point people to relevant areas on the website, increasing content consumption and delivering a better service to the public. From experience with other government customers, this can have a positive effect on reducing incoming calls from the public (self-service) freeing up CQC resources and saving the organisation money.

User Stories

SUBSCRIPTIONS

Website user/subscriber

6. As a website user, I want to be able to sign up to receive a range of newsletters using a webpage on the CQC site so that I can stay in touch with updates on the subjects that matter to me.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    Please see the section "Overview of the sign up process" for a detailed answer to this question.

7. As a website user, I want to be able to indicate my areas of interest on the sign up page, so that I can receive alerts when new information about those areas is published on the website.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    In addition to the detailed response shown in the previous question, the GovDelivery service uses extremely flexible automation tools to conserve resources and improve organisational efficiency.

    The innovative "PageWatch" technology monitors clients' online channels for content update and then sends messages to subscribers when certain predefined automation actions apply for each topic. This would enable ad hoc emails about key publications at the time of publication, e.g. State of Care (rather than waiting a week or more to put the news in a scheduled newsletter).

29

8. As a subscriber, I want to be able to unsubscribe from a given newsletter by clicking a link at the bottom so that I can easily cancel my subscription.

9. As a subscriber, I want to be able to view and edit my current subscriptions by clicking a link in a mailing sent to me so that I can add and remove sign ups or simply see what the current options are.

   The GovDelivery Communications Cloud service is fully compliant with these two objectives.

   Users can unsubscribe at any time by clicking a link within an email which will take them to their 'subscriber profile' and allow them to delete their profile and/or manage their individual subscriptions. This enables users to be in complete control of their subscriptions.

   Below is a copy of an email alert from CQC which clearly demonstrates the ease at which the subscriber can edit or cancel their subscription within the bottom footer section.

Editor

12. As an editor, I want the sign up page on the website to link with the subscriber database so that we can deal with sign-ups automatically rather than needing manual intervention.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    All subscriptions are managed from the CQC website via the GovDelivery system and entered automatically into the email management system; no manual intervention from CQC will be required.

    All subscribers will have the ability to fully manage their subscription profile online and can add and delete subscriptions, manage subscriber preferences and remove accounts. However, subscriber details can still be entered manually by CQC if needed e.g. if need to upload subscriber lists from other sources.

13. As an editor, I want to be able to add, edit or remove entries in the subscriber database so that I can make changes for people unable to use the form or test subscriptions.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    CQC administrators can manage all subscriber options and preferences from our secure web based interface. Authorised Editors/Administrators can edit, add or remove entries in the subscriber database. An audit trail is retained of who logged in and amended the record.

14. As an editor, I want to be able to add and remove options to the sign up page and have these populate fields in the subscriber database so that I can easily launch new bulletins without the need for development work.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    Via the secure administrator interface, authorised Editors/Administrators can quickly edit, add or remove bulletins in the CQC "Topic" list. This enables editors to be able to add and remove bulletins simply and quickly, and as frequently as they like, without the need for external intervention or development work.

    There is no limit to the number of topics that can be offered by CQC and an audit trail is retained of who logged in and amended the topic list.

15. As an editor, I want to be able to set the page where subscribers are redirected to once they have submitted the sign up page on the website so that I can manage their journey and use a page with other ways to stay in touch advertised.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    The system can be configured to set the page subscribers are redirected to once they have submitted the sign-up page. In this way, CQC will be able to manage the subscriber's journey and can provide them with information on other ways to stay in touch with CQC.

16. As an editor, I want to be able to query the database to get lists of subscribers to particular mailings so that I can use these to send newsletters or mailings to.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Due to the granular nature of GovDelivery subscriptions providing details of which subscriber is subscribed to which mailing is very easy. CQC will be able to use this information to filter sends, create new lists and segment audience for new bulletins and messages.

17. As an editor, I want to be able to download spreadsheets of subscribers in Excel format for use outside the tool so that I can use this information elsewhere or compare it to other data.
The GovDelivery Communications Cloud service is fully compliant with this objective.

Administrators can easily import or export subscribers at any time via the user interface. Subscriber email addresses can be imported or exported in CSV/Excel format.

18. As an editor, I want to be able to upload Excel spreadsheets of email addresses to receive a particular mailing so that I can quickly take information from the CRM system and use it to send out a mailing.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Administrators can easily import or export subscribers at any time via the user interface.
*Subscriber email addresses can be **imported or extracted in CSV format**. The image below illustrates the area within the interface where subscribers can be added/removed.*
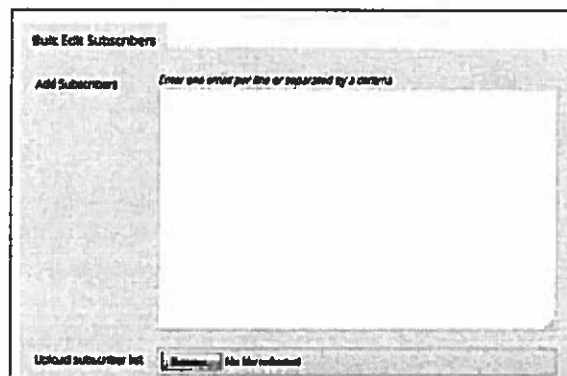
Figure: Subscriber details can be added manually or uploaded via CSV files. An audit trail is retained of who logged in and amended the record

19. As an editor, I want to be able to upload spreadsheets of names, email addresses and subscription information so that I can quickly make changes to large numbers of lines in the database.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Administrators can easily import or export subscribers email addresses along with other metadata such as "First Name", "Occupation" etc. at any time via the user interface.

*Subscriber email addresses and other data can be **imported or extracted in CSV format**.*

BUILDING NEWSLETTERS

Editor

20. As an editor, I want to be able to add new html templates to the tool, both for complex newsletters and simple letters, so that I can redesign any of the mailings at any point.

The GovDelivery Communications Cloud service is fully compliant with this objective.
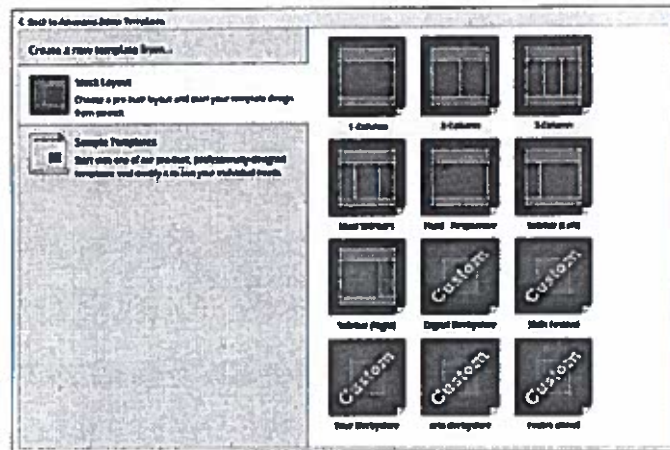
Figure: Many options available including the ability to select from various pre-created template themes.

Communications Cloud offers the ability for users to create, edit and manage multiple newsletter templates, both complex and simple. Newsletters can be created using a simple WYSIWYG editor which is extremely simple to use being 'drag and drop'. There are multiple options in terms of design including single, two column, sidebars etc. Templates can be custom designed to enable them to render correctly on mobile devices and tablets.

The templates have been tested on all major email clients to render correctly.
All aspects of the template can be modified by a template editor including images, hyperlinks, dividers, fonts, background colours, padding, text size and many other features. Creators can also stipulate what areas are fixed or variable to keep the design consistent. Within the editor there is the option to have responsive templates to cater for subscribers opening messages on mobile devices and tablets.
Below is a screenshot of the Newsletter editor.

Figure: WYSIWYG editor used to create newsletters.

21. As an editor, I want to be able to create new issues of an email or newsletter (usually by copying past templates) so that I can quickly add each month's issue of a given newsletter.

The GovDelivery Communications Cloud service is fully compliant with this objective.

The service offers the ability for users to create, edit and manage multiple newsletter templates. Newsletters

*can be created using a simple **WYSIWYG** editor which is extremely simple to use being
'drag and drop'. Newsletter content can be copied and paste from other sources e.g. MS Word and inserted*

into the correct location in the newsletter template.

These templates can be stored for future use. All aspects of the template can be quickly modified via the template editor including images, hyperlinks, dividers, fonts, background colours, padding, text size and many other features.

Creators can also stipulate what areas are fixed or variable to keep the design consistent.

Within the editor there is the option to have responsive templates to cater for subscribers opening messages on mobile devices and tablets.

22. As an editor, I want to be able to use a wysiwyg interface to easily edit the words, pictures, links, font, font colour, font styling of existing templates so that I can still create a new version of the template even if I know little about html.

The GovDelivery Communications Cloud service is fully compliant with this objective.
The Newsletter tool has been designed for non-technical users who do not understand HTML. Communications Cloud offers the ability for users to create, edit and manage multiple newsletter templates. Newsletters can be created using a simple WYSIWYG editor which is extremely simple to use being 'drag and drop'.

There are multiple options in terms of design including single, two column, sidebars etc. Templates can be custom designed to enable them to render correctly on mobile devices and tablets.

All aspects of the template can be modified by a template editor including images, hyperlinks, dividers, fonts, background colours, padding, text size and many other features.

Creators can also stipulate what areas are fixed or variable to keep the design consistent. Within the editor there is the option to have responsive templates to cater for subscribers opening messages on mobile devices and tablets.

23. As an editor, I want to be able to have an online version of the newsletter created automatically so that I don't have to host the html somewhere on the live site.

The GovDelivery Communications Cloud service is fully compliant with this objective.

All messages sent via Communications Cloud have the option of providing a public "landing page" which provides a hosted (by GovDelivery) web page of the message that was sent.

24. As an editor, I want to be able to create a plain text version of the newsletter so that users who only accept text email can still read the newsletters.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Plain text versions of the newsletter are created automatically by the GovDelivery system and sent together with the HTML version using the MIME Multipart message format. This ensures messages render correctly on the subscribers chosen platform and also work correctly with screen read.

25. As an editor, I want to be able to create other formats, e.g. print and pdf versions so that I can save or print the newsletters easily.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Bulletins can be created in HTML and plain text formats. As GovDelivery is a web-based system, Newsletters and Bulletins can be printed or saved from the administration interface as PDF versions using web browser features.

26. As an editor, I want to be able to add an attachment to a mailing so that I have the option of including documents with a bulk email.

The GovDelivery Communications Cloud service is fully compliant with this objective.

The GovDelivery Communications Cloud service will allow CQC to attach documents to bulk email but this is not in keeping with our best practices.

However, the GovDelivery service offers a hosted online area where documents can be stored and accessed by subscribers when CQC notifies them of their availability and forwards the download URL. This removes the requirement to send bulky mails which may temporarily fill up the subscribers in box and also impacts deliverability rates.

By including a link to a download area, GovDelivery tracks clicks and downloads of each attachment which will help CQC measure engagement and user activity.

27. As an editor, I want to be able to use 'mail merge' type features to include variable text in a given place, including where one email address is shared across multiple lines of data, so that I can personalise mailings to the recipients by including names, company names etc.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Metadata for mail merge functionality can be stored in the system as "question data" is asked during the subscriber   sign   up
process.

Macros can be placed within message templates to automatically pull in information including "Names" & "Company names" etc. when messages are sent to the subscriber.

28. As an editor, I want to be able to easily preview mail-merged emails so I can check for errors before sending.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Mail-merged messages can often run into the 1,000's so having the facility to preview a large number of emails ahead of a send is not feasible and heavily resource intensive. The data that can be used to populate this information can be easily downloaded by administrators and manually checked should this be required.

The best practice approach to previewing and test sending mail-merged messages would be to use a small, internal distribution list which can be used to receive actual sends and verify the information to prove the mail merge is working correctly. Once tested the full merge on large subscriber lists can be run.

29. As an editor, I want to be able to save copies of each issue of a newsletter so that I can refer back to them in future.

The GovDelivery Communications Cloud service is fully compliant with this objective.

All messages sent to subscribers are archived in the GovDelivery Communications Cloud service. Commonly used messages can be saved as templates for future use.

30. As an editor, I want to be able to tag links for campaign tracking purposes, e.g. to see how many clickthroughs on a particular link.

The GovDelivery Communications Cloud service is fully compliant with this objective.

The service comes with a complete set of analytical tools which can be accessed by administrators via the secure user portal. This functionality will allow CQC to measure a large range of metrics including full link tracking and activity for all links across all messages.
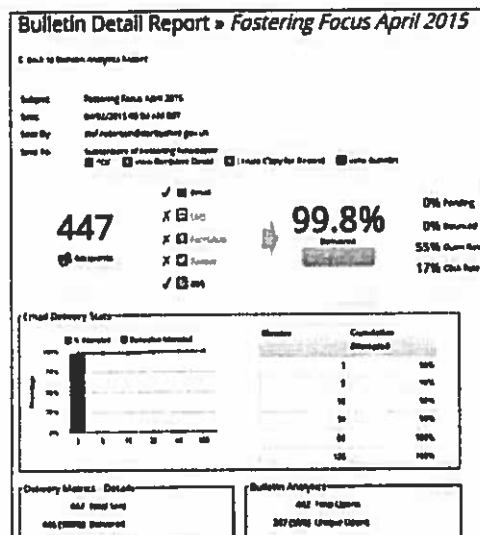
Figure: Screen showing newsletter performance including open and click-through rates.

Administrators sending a message can opt to receive a detailed delivery report (sent 4 hours later) straight to their inbox giving an accurate snapshot of the message performance including number of recipients, channels used, delivery rate, opens, clicks, unsubscribes, links clicked and other stats.
An example of a typical message analytics report is illustrated on the right.

In addition to the comprehensive range of reports available within the admin interface, GovDelivery have a Business Intelligence team who are happy to work with clients to create bespoke reports to satisfy additional business requirements

31. DESIRABLE: As an editor I want to be able to do A/B testing to establish the best messaging / design etc. for a mailing before sending it to the entire subscriber base.

The GovDelivery Communications Cloud service is fully compliant with this objective.

A/B tests within the GovDelivery Communications Cloud Licence allow admins to manually send two different messages to subscribers and track which message subscribers better engage with to optimise results.
As standard, admins can manually run A/B tests by creating two different versions of a message and use the criteria within the system to select a random audience size for the messages, go back into the system after a time period, analyse the results and then determine which message should be sent to the bulk of subscribers.

The manual process described above often requires time and resource to create, apply filters, analyse and make final sending decisions at a later date therefore the optional GovDelivery Professional Licence incorporates an automated A/B Testing module to allow for seamless A/B testing to take place. An intuitive and easy to work with workflow allows admins to pull in different message versions from the editor, choose the test run length, and choose whether the better performing message should be automatically sent to subscribers.

Figure: A/B Test Campaign workflow within the Professional Licence

The A/B Testing functionality within this package incorporates two elements: "50/50 Test" and "Test and Send". The 50/50 Test allows admins to send two variations of a message to an equal split of subscribers – ideal for testing the overall look and feel of a template where you wish to determine which style in the most engaging. Given templates are not changed on a regular basis, this is an important feature to ensure maximum engagement with any given design.

The Test and Send functionality is the more traditional A/B test functionality which is designed to be used on a more frequent and regular basis. For example, a regular newsletter where image placement/type and/or subject lines can be tested.

GovDelivery clients using this element of the Professional Licence are able to more frequently use A/B testing, optimise efforts and the engagement with messages, and save time by setting up a campaign and letting the system analyse data and automatically triggering the right message based upon the agreed success criteria.
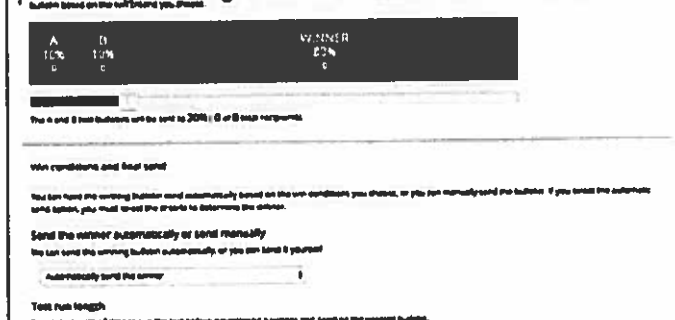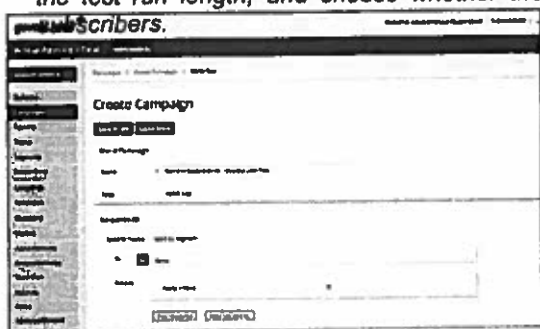
Other Communications Cloud users using the Professional package have reported up to a 25% increase in open rates, and 10% increase in click rates by consistently streamlining and automating A/B tests of key messages.

CQC have the option of taking advantage of this to drive greater and deeper engagement with their communications. This greater engagement would have a direct impact on web traffic, content consumption, and ultimately drive more action and better outcomes from subscribers.

SENDING

MAILINGS Editor

32. As an editor, I want to be able to set the address the email comes from, the alias of the sender and a cqc.org.uk address that replies or bounce backs are forwarded to so that I can control the way the newsletter appears in recipients' mailboxes.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    GovDelivery will utilise clear and consistent "from" names and "from" addresses in email bulletins, so subscribers know the messages are coming from CQC. Bulletins will take on the CQC's look and feel so that they will appear to be coming from CQC.

    GovDelivery provides automated bounce handling to manage all synchronous and asynchronous email bounces resulting from hard failures (e.g., invalid email address) and soft failures (e.g., mailbox full and other transient errors). GovDelivery can designate a central email where all replies are sent to.

33. As an editor, I want to be able to set the subject of the email so that I can control what the newsletter will be called when it is received.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    CQC will have complete control over the newsletter subject line. We also provide support for message "pre-headers" so that a brief description of the message content is displayed on mobile devices.

34. As an editor, I want to be able to preview what the newsletter will look like before sending it so I can be assured that the layout is complete.

    The GovDelivery Communications Cloud service is fully compliant with this objective

    A web based preview is provided for newsletter editors and the system supports the ability to send test sends to multiple recipients should CQC wish to implement internal approval processes.

35. As an editor, I want to be able to use a suppression list to remove some subscribers from a mailing so that I can prevent people receiving newsletters even if they are subscribed to them.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Please note, we do not need to use suppression lists as a means of maintaining SPAM scores due to the unique way we manage ISP relationships.

   CQC administrators are able to drill down and, through the use of filters, decide which of the subscribers subscribed to any given topic will receive the bulletin.

36. As an editor, I want to be able to limit the deployment of a mailing so that I can ensure all recipients don't all get a particular mailing at the same time (and therefore all hit our website at the same minute).

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   The current sending volumes and methodology used by CQC within GovDelivery ensures this event hasn't been experienced.

   CQC Administrators can limit the deployment of a mailing so that all recipients don't receive a bulletin at the same time. Currently, this is not automatic, so you would need to manually send each mailing. For example, if you wanted to send only 25% of the mailing at a time, you would need to manually send the bulletin four times using the filters available.

37. As an editor, I want to be able to view the details of any subscribers suppressed from a mailing to protect the spam score so that I can see who is not receiving it.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   As had been proven, email delivery rates at CQC are very high due to our unique way of managing messages for the public sector which eliminates the need for SPAM scoring. GovDelivery provides a detailed report of all subscribers that have unsubscribed from the service as a result of marking CQC messages as SPAM either directly or via ISP feedback loops.

   GovDelivery works hard with the major ISPs to ensure that emails originating from GovDelivery servers are not treated as SPAM. Therefore, emails sent by GovDelivery will not have any adverse impact on CQCs SPAM score.

   There is no mailing suppression functionality as outlined in the previous question. A suppression list is held at account level which will prevent previously unsubscribed subscribers from being uploaded to topics.

   The Communications Cloud has robust reporting capabilities, which allows CQC to access important metrics and analytics at any time.

38. As an editor, I want to see the number of recipients before I send a mailing so that I do not prematurely send out a bulletin to a large number of people.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   As soon as the "Topic" groups have been selected to receive the message and before sending to subscribers CQC are able to review all aspects of the message including a "Live" recipient count. The decision can then be made to send by the editor.

39. DESIRABLE: As an editor, I want to be able to configure automated email campaigns to prompt people to take certain actions after a given time period (e.g. one month after subscribing or one year since last updating details) so that I can encourage subscribers to engage more with our products without sending manual emails.

The GovDelivery Professional Licence is fully compliant with this desired objective.

A key element of the Professional Licence is the ability to create, configure and automatically send campaign messages to subscribers.

Re-engagement campaigns can be configured to reach out to subscribers who are inactive or sleepy.

Managing large and rapidly growing lists has its challenges when it comes to maintaining engagement with subscribers and routinely identifying individuals who are not interacting with your communications.

By setting up drip campaigns within the GovDelivery system, unengaged subscribers can be automatically identified and emailed at given time periods to nudge/encourage them to take action. This could be the cross-promotion of other CQC products or services, or simply to update preferences and subscriptions. By running these types of campaigns throughout the year, organisations are able to improve the overall health of subscribers and achieve better outcomes and results, without spending valuable time on a weekly/monthly basis manually sifting through data to identify, analyse and manually send messages to these subscribers.

1 IDENTIFY STALE SUBSCRIBERS
Subscriber who have gone inactive or haven't opened or clicked on your messages

2 RE-ENGAGE
Subscriber receives a message with new information, with suggested content

4 ANALYSE AND IMPROVE
Review what topics or messaging increases subscriptions and decreases inactivity

3 CROSS-PROMOTE
Subscriber receives cross-promotional content with new, relevant, or similar topics of interest

Figure: Re-engagement campaign workflow within the Professional Package

Welcome/on boarding campaigns can be easily created within the system to allow automatic engagement with subscribers after initial sign up. Creating a positive first impression is key to maintaining good engagement with new subscribers. By being proactive and engaging with new subscribers at set periods after sign-up, CQC will have the ability to create more value with subscribers, better promote additional and relevant goods/services, and achieve better message opens/clicks by forming a positive relationship from the outset.

These campaigns can consist of multiple messages, each with their own set send schedule based on various criteria, allowing CQC to drill down and better target its subscribers. Once created and triggered, a campaign requires to manual intervention or resource by CQC.

Reporting within the system will give CQC insight into how each campaign is performing, detailing subscriber engagement and action, open/click rates, and link tracking giving the business insight into what kind of interactions are taking place with sent emails.
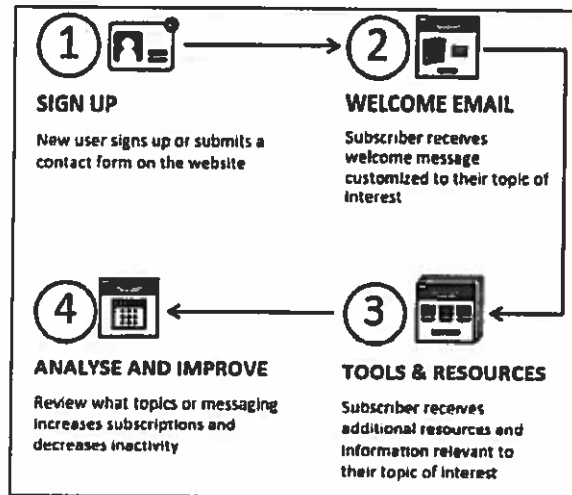
Figure: Welcome/ on boarding campaign workflow within the Professional Package

The IPO (Intellectual Property Office) are using the GovDelivery Professional licence to run drip campaigns to support their ministerial target around new engagement with UK SME's. The distinct messages allow the IPO to save time and resource, with the system identifying groups of subscribers who have/have not taken action, and messaging accordingly through the campaign to increase engagement.

40. DESIRABLE: As an editor, I want to be able to send emails to segments of lists based on audience interests, so I can make emails are relevant for the recipient.

The GovDelivery Professional Licence is fully compliant with this desired objective.

Segments allow you to group subscribers using multiple, granular criteria to better refine your communications and save time.
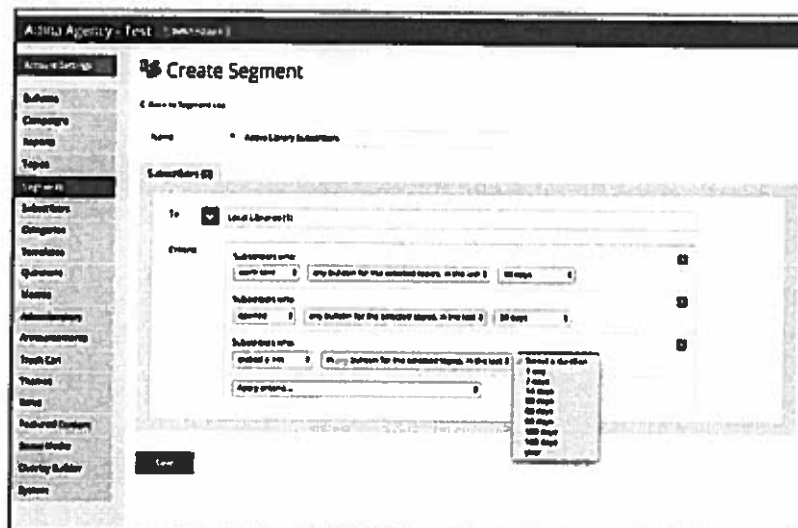
Figure: Creating segments within the GovDelivery Professional Package

While filters can be used manually within the existing, basic licence, it is a very time consuming process to continually create and verify sending filters at the time a message is sent. Large numbers of unique dynamic segments within the Professional licence can be set up and forgotten about; leaving CQC to focus on other tasks and save administration and time.

Multiple segments can be created which update dynamically based on changes in subscriber activity and can comprise of various other criteria within the account.

39

These segments can be used within campaigns and sent messages which are highly targeted based on specific activities.

STATISTICS AND TRACKING

Editor

41. As an editor, I want to be able to see statistics easily for subscriber numbers so I can easily understand the database size and popularity of the mailings.

42. As an editor, I want to be able to track all the normal email statistics – delivered, opened, forwards, any click, clicks for each link in the message, soft bounces, hard bounces, unsubscribes, device used to view, etc. and have clear definitions for these – so that I can prepare reports on the use of the newsletter by subscribers.

43. As an editor, I want to be able to track the email statistics by the particular issue I was sending out or by a given time period so that I can understand use over time.

*For ease, we have combined the response to the above three questions regarding **Statistics and Tracking**, into one answer below which covers all three aspects.*

The GovDelivery Communications Cloud service is fully compliant with these three objectives. Communications Cloud reports provide real time management data specific to the activity completed in your account. You see the impact of your multi-channel communications efforts in a timely manner.

You can go beyond just who you communicated with, to analysing who opened, clicked on, and shared your information - this provides a much better view of actual audience engagement with your messages, as well as growth of your subscriber lists.
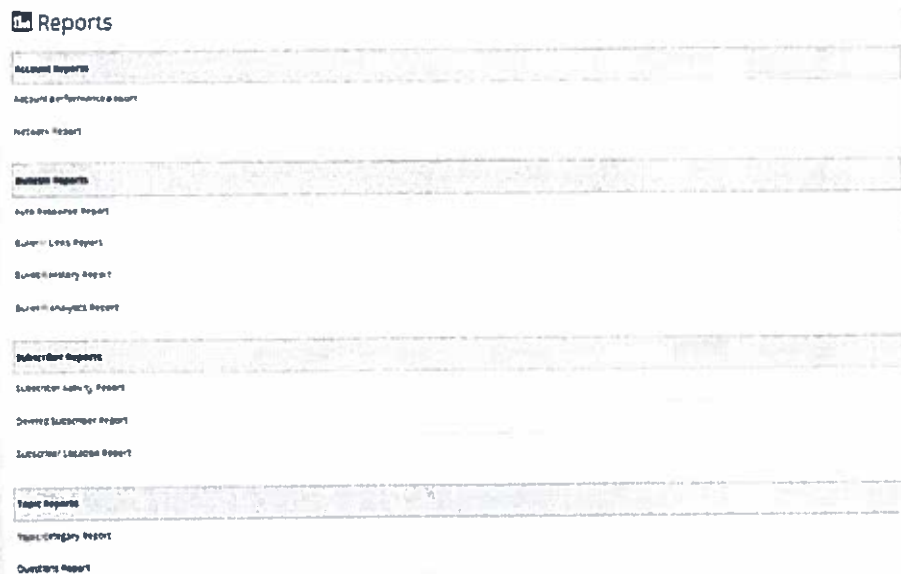
Figure: Comprehensive Management reports available in Communication Cloud.

The vast majority of reports are displayed as graphical dashboards that provide a visual representation of the Management Information although all data can be exported via CSV or into MS Excel if required. Example dashboards

are shown below.

Figure: GovDelivery records app... tionality will allow you to target and segment subscribers based on their location.

Accounts Reports

Account Performance Report: provides a comprehensive twelve-month snapshot of success metrics for your organisation.

Network Report: shows how many subscribers are added to your account through participation in the GovDelivery Network.
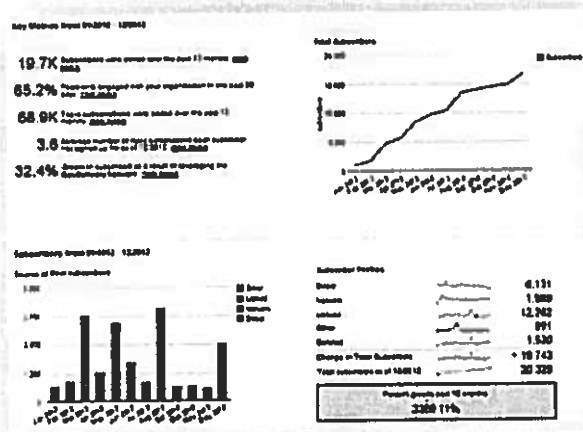
Figure: Account management reports show detailed information on subscriber metrics.
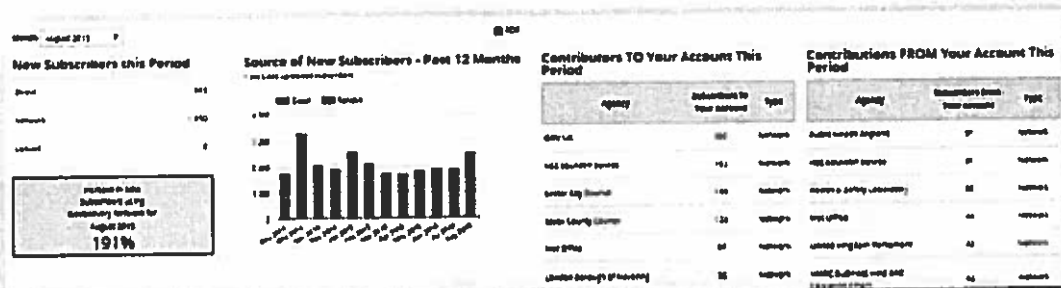
Figure: Network report showing the source of your subscribers together with your most effective netw

Figure: A recently sent message from the CQC GovDelivery account

10. As a subscriber, I want to be able to sign up to receive a text-only version of newsletters so that I can get a version more easily understood through a screen reader.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   - *All messages are sent as MIME Multipart messages meaning both HTML and plain text messages are delivered simultaneously so they can be displayed in the correct format on the receiving device. This approach requires less work for CQC and helps the message display correctly on more devices.*

11. As a subscriber, I want to be able to click a link to view the mailing online so that I can see it properly if my email programme doesn't display it.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Messages can easily be configured to include a web "landing page" which will allow the recipient to view a web version of the email message should the email not display correctly. The landing page also allows people to share the message across social media channels.

   The screenshot above contained within response 9/10 shows the existing "click here to view online" feature within CQC messages.

Bulletin Reports

SMS Subscriber Report:
   o *Provides details on bulletins sent to CQC's SMS subscribers.*

Bulletin Links Report:
   o *Details links included in bulletins and the click rates for those links.*

Auto Response Report:
   o *Details all Auto Response activity for CQC. Note that the Auto Response report is only available if Auto Response is enabled for your account.*

Bulletin Analytics Report:
   o *A complete listing of all bulletins sent by CQC and detailed delivery and response tracking metrics. Note that you must have Bulletin Analytics enabled to see the Bulletin Analytics report.*

Bulletin Detail Report:
   Shows the performance of an individual bulletin, such as a newsletter.

Figure: Subscriber/ Subscription management reports show detailed information on subscriber metrics.
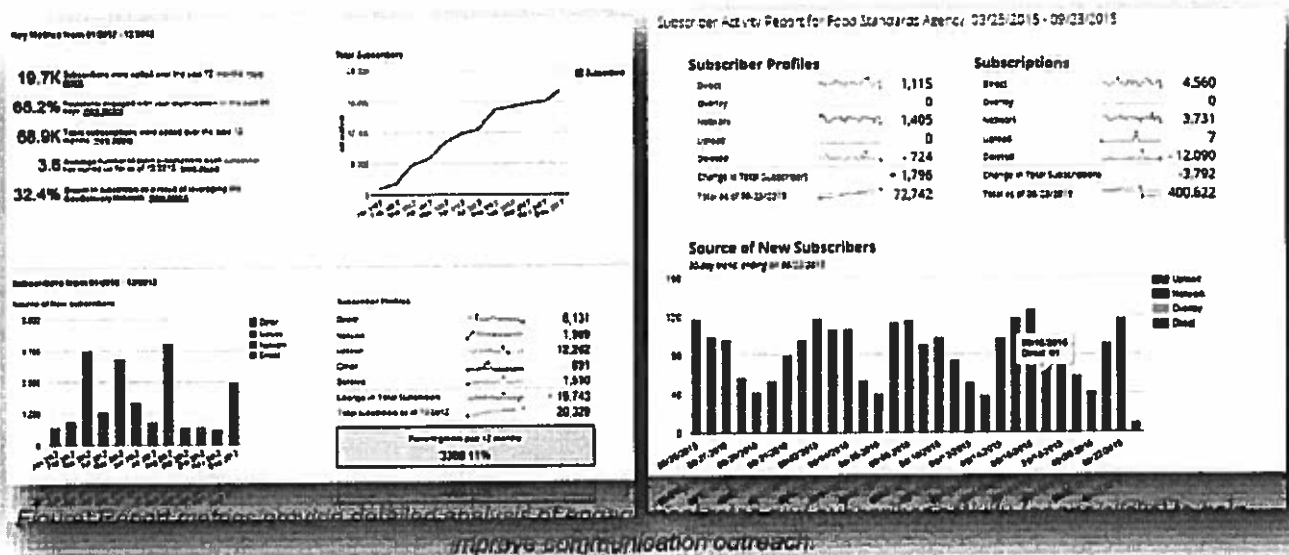
Subscriber Reports

- Subscriber Activity Report: displays the number of subscribers for your account and provides a historical picture of subscriber counts.
- Deleted Subscriber Report: provides details on when, why, and by whom a subscriber profile is deleted.

Questions Report:

Provides summary and detailed reporting for the questions that you ask subscribers during the subscription process.

Topic/Category Report:

Details topic and category activity for your account during a selected time range.

MANAGING PAST MAILINGS

Administrator

44. As an administrator, I want to be able to create, edit and delete folders in which to store mailings and templates so that I can organise the library of past issues easily.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Due to the granular nature of the Communications Cloud system, message templates are created centrally in the system and then assigned to specific topics/newsletter categories. This approach means newsletters are automatically allocated to the correct "folder".

   Sent messages are managed in exactly the same way, with an archive of each message sent to a specific newsletter topic/category stored within the category itself. This allows messages to be resent and reused quickly and efficiently.

45. As an editor, I want to be able to search, filter and sort the mailings so that I can find the previous issues I am looking for easily.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Administrators can easily search and filter by message subject line, sending admin, in addition to date range.

46. As an editor, I want to be able to export a html and pdf version of a mailing so that I can save a copy outside of the tool easily.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Communications Cloud is web based and hence the ability to provide PDF versions of message utilises browser features to achieve this functionality.

   Messages can be edited in HTML format and copy-and-paste into other applications as required from the message source.

MANAGING ACCOUNTS

Administrator

47. As an administrator, I want to be able to create, edit and remove user accounts for people needing access to the system so I can enable new staff to be trained and old accounts to be closed.

48. As an administrator, I want to be able to restrict the access people have to particular areas of the tool so that I can limit what content and templates they can edit.

49. As an editor, I want to be able to request a password reset so that I can gain access again after I have forgotten my password.

   The GovDelivery Communications Cloud service is fully compliant with these three objectives.

   For clarity and ease we have combined the response to the above three questions regarding Managing Accounts, into one answer below which covers all three aspects.

   The GovDelivery platform allows for self service provisioning/de-provisioning via privileges applied to user roles. Administrators, with the appropriate administrative privileges can provision capabilities and features such as creating additional topics for subscriptions, managing other lower level administrators, web service integrations, outbound communication across multiple channels, and a full range of reporting capabilities.

- Account Administrator – Access to all account functions including the ability to create new newsletter topics, create, edit and remove user accounts for people needing access to the system and limit what content and templates they can edit. They also have the ability to set & change passwords as well as send messages.

- Category Administrator – Access to a subset of functions to support management of all newsletters within a specific area. Functions include the ability to create new Category and Topic administrators within the specified category, create and amend topics associated with the category, change passwords and create/send messages.

- Topic Administrator – Ability to create and send messages / newsletters.

- Report Viewer – Access systems to reports only.

An Account administrator can restrict access lower level/topic admins have to certain areas including templates/topics/reports.

All admins can at any time request a new password to gain access if it is forgotten.

Non Functional Requirements

Availability requirements & support

50. System availability – Any system is required to meet service availability levels of 99.5% Monday to Friday 5 days a week, with the exception of bank holidays, with system maintenance outside working hours.

The GovDelivery Communications Cloud service is fully compliant with this objective.

GovDelivery has historically achieved over 99.5% availability (99.9% in 2017) of its website and services. Website availability is defined as the ability of users to access the GovDelivery website and the Services via the Internet.

51. Disaster recovery – System will be supported in the event of a disaster and any recovery plans will be tailored to CQC needs and be compliant with business continuity standards.

The GovDelivery Communications Cloud service is fully compliant with this objective.

GovDelivery maintains two secure data centres which provides fail-over support. We will be happy to share our plans with CQC if required and discuss specific CQC requirements.

Recovery Time

52. Recovery time & point objective – Minimal recovery time with optimal recovery points.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Please see below for an overview on recovery procedure. The recovery time depends on the severity and extent of any given instance. If restoration of data is required.

53. Backup schedules - Back-ups are to be carried out completely according to the documented data back- up requirements. Appropriate personnel are to verify the usability of backed-up data and retain verification evidence.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Each night, full back-ups are written to enterprise-class storage. Each week, full operational back-ups (excluding historical data) are secured offsite. Back-ups are retained for one year and then destroyed.

In the event of a problem with any production hardware, the immediate goal will be to fix that problem and return

the production server to use. In the case of the application servers, the system would run on serviceable servers while the down server is being repaired. In the case of a database server, fixing a problem with the production server could involve the restoring of data from the standby server or the substitution of hardware from the standby server.

If these measures are impractical, we will place the standby server in production. In the event of a catastrophic problem that requires the commissioning of either new hardware or servers, the general procedure is to configure the new server to standard build, place the new server on the network, install basic software, and restore from disk back-up file.

Performance & scalability

54. Storage - System must handle increase in database and report server storages without major system changes or data migration activities.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    One of the key features of a Software as a Service, solution is that all aspects of scaling and storage is the responsibility of the supplier and as such are covered in the monthly fee.

    Any increases in storage or servers in our service will have **no impact** and will be invisible to CQC. Please note that GovDelivery does not charge per email or per Mb. We have a flat monthly fee which is fixed throughout the annual contract irrespective of the number of emails sent.

55. System scalability - System shall be scalable both in terms of users and storage, with easy to change both in terms of cost and minimal disruption.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    One of the key features of a Software as a Service, solution is that all aspects of scaling and storage is the responsibility of the supplier and as such are covered in the monthly fee.

    Any increases in storage or servers in our service will have **no impact** and will be invisible to CQC.

56. System performance - Describe the typical response time that can be expected from an end user perspective when accessing the application.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    GovDelivery is used by over 175 million users worldwide. The service is web-based and hence when a subscriber (or administrator) accesses the system they receive an immediate real-time response.

Monitoring

57. Application monitoring - The application must be monitored by the provider, with suitable alerting tools in place to notify of current or imminent service breaches + security issues.

    The GovDelivery Communications Cloud service is fully compliant with this objective.

    As part of our ISO27001:2013, FedRAMP and UK government accreditations (previously IL2) the application is constantly monitored by a number of processes to ensure it is functioning correctly.

    This is assured via industry leading equipment and software tools which monitor the applications and alerts the support engineers instantly should there be a current or imminent service breach or security issue.

    The applications are run on several devices inside our secure geographically distributed datacentres to allow for redundancy in the event of a hardware failure, or failover in the event of power outage etc.

    In addition, there are several layers of hardware and software defences in place to protect against cyber-attacks.

GovDelivery application and datacentres are evaluated by a third-party company certified to carry out such assessments.

As part of the GovDelivery security posture, GovDelivery is unable to disclose in detail its security procedures until a None Disclosure Agreement (NDA) has been signed and approved. Under the terms on the NDA, GovDelivery would be happy to discuss in more detail its security posture with CQC

Reporting

58. Availability reporting – Required by exception (where there are system outages)

The GovDelivery Communications Cloud service is fully compliant with this objective.

We will provide appointed CQC administrators with alerts and notifications if a system outage is identified. During an outage, frequent reports/updates will be provided given an indication of the issue, remedial action being taken and anticipated resolution times.

It is the responsibility of the Customer Service manager to ensure client communication is maintained during an outage.

Change management and release process

59. Change management – Communicate in a timely manner any planned changes to the system / software and how users will be affected

The GovDelivery Communications Cloud service is fully compliant with this objective.

Scheduled maintenance typically occurs every 30 days with average downtime required being less than 30 minutes.

Planned or routine maintenance is limited to 2 hours per week on Sundays between 12:00 am and 3:00 am Pacific Time.

We reserve the right to change the schedule downtime to other non-business hours upon a 24-hour notice to CQC. Scheduled Downtime shall not be considered times when the system is unavailable. Total scheduled downtime for the year will not typically exceed 20 hours.

60. Release Management – Communicate timelines for any planned releases in a timely manner

The GovDelivery Communications Cloud service is fully compliant with this objective

All customers, including CQC, benefit from standard releases with no cost to CQC, unless a specific cost-based feature is desired. Summaries of version updates and releases will be communicated to CQC.

Our service has been designed so product updates can be deployed in real-time without the need for any service down-time for the upgrade. However, we do maintain a published release schedule as described above. Any down-time outside this schedule will be communicated to CQC with at least 24 hours' notice.

Security

61. Hosting - System shall be capable of being hosted either on cloud site or on the supplier premises. If on cloud it must be capable of hosting to ISO27001.

The GovDelivery Communications Cloud service is fully compliant with this objective.

GovDelivery Communications Cloud is a Software as a Service application. We maintain current ISO 27001:2013 certification and are certified Tier III by the Uptime Institute.

62. System must also be demonstrably capable of data security standards up to and including IL2 data.

The GovDelivery Communications Cloud service is fully compliant with this objective.

We provide a highly secure service that greatly exceeds UK government security requirements. GovDelivery holds full IOS27001:2013 accreditation and we have previously been audited and accredited as an IL2 secure data centre by CESG as part of an ongoing project with HMRC.

It should be noted that providers are no longer required to hold IL accreditation (which is now a defunct security standard) although we have consistently passed G-Cloud and other government security audits to verify the equivalent of IL2 security levels.

63. Access control - System shall support 1 x user account per user. System shall be demonstrably capable of segregating access to functions and data based on roles or specific users.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Only 1 user account per user is permitted in the system (managed via registered email addresses). Each user is

   allocated role-based permissions that provide access to only permitted areas of the Administrator system.

64. Audit - The system shall be capable of retaining an audit trail for user interactions / events for a period of at least six months that is easily accessible and available on request by CQC.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   We will keep a complete archive of GovDelivery Communications Cloud data created by CQC, including message sends, audit trail and subscriber history for 18 months (rolling).

Identity & access management

65. User management - Procedures are in place to ensure timely actions in relation to requesting, establishing, issuing, updating, suspending and closing user accounts.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Account administrators can make these changes at any time via the secure user portal. CQC will be able to manage this entire process without the need to contact GovDelivery.

66. Formal approval of user changes - All user account and access management actions e.g. creating, amending, removing, require formal change control approval.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Account administrators can make these changes via the secure user portal. CQC will be able to manage this entire process without the need to contact GovDelivery.

67. Account lock out - The number of failed login attempts before system lockout is 3 attempts or less.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   CQC will have the facility to set the number of failed login attempts before system locks-out.
   By default, an administrator's account is locked for 30 minutes after three unsuccessful login attempts from the same user ID and IP address within 5 minutes.

   Once an account is locked, we will not send any communication to the administrator. To unlock the account, the administrator must do either of the following:

   - *Wait 30 minutes and attempt to re-login.*

- *Immediately reset their password via the link on the login page which sends an email to the authorised email account for that user.*

68. Database access restrictions - For applications that have a separate database (e.g. Sql Server or Oracle) access to the database must be restricted to appropriate and authorised personnel only. For applications that have a separate database (e.g. Sql Server), database accounts and their roles/groups are reviewed periodically for appropriateness.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   CQC staff are only able to access the service via the web-based administration interface. No direct access to the database is provided.

69. Change default passwords - For applications that have a separate database (e.g. Sql Server, Oracle), default database accounts will be disabled/removed or the passwords changed.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   CQC staff are only able to access the service via the web-based administration interface. No direct access to the database is provided.

70. Data ownership - All data within the system must be defined and have a documented owner.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   All data held in the CQC account is owned by CQC and will not be used by GovDelivery, or shared with any third parties.

71. All CQC data must be capable of being returned to CQC, in a usable format, in the event of termination of the contract.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Should CQC decide to terminate the contract, GovDelivery will return all the data uploaded from CQC and all the data collected via the CQC Communications Cloud account, to CQC in a CSV file free of any charges.

Confidentiality & integrity

72. Confidentiality & integrity - The system will maintain data integrity standard up to and including IL2 throughout the data lifecycle. The system should be fully protected against malicious code with automated checking of all emails / data sent out.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   Data integrity will be maintained at all times and will be managed under the terms of our ISO27001:2013, FedRAMP and UK government security requirements. The system is fully protected from malicious code and maintains active Intruder Detection Systems (IDS) and other industry best practice security principles.

   We do not permit any codes/scripts to be inserted into either emails, messages, or user interfaces used by the system.

Usability

73. Language support - The application must support UK English only.

   The GovDelivery Communications Cloud service is fully compliant with this objective.

   The GovDelivery service is delivered in English. When editing and creating text for bulletins the service uses the local device' dictionary to spellcheck message content.

74. Desktop support - All system configuration settings are accessible to system administrator through application screens or setup programs (i.e. no hard coded system variables exist and include system, user, roles, company and other configuration screens).

The GovDelivery Communications Cloud service is fully compliant with this objective.

GovDelivery is a SaaS service. No desktop applications or setup programmes are used. All system configuration settings are accessible to system administrator through our web based application.

75. Software as service - Customer Desktop devices are restricted in terms of the ability to download components from external sources. The system shall operate with the minimal need for software components to be applied to PC or desktop devices.

The GovDelivery Communications Cloud service is fully compliant with this objective.

The Communications Cloud is a web-based, software as a service solution that does not require hardware or software to be installed on any CQC server or computer.

Compliance

76. Legal compliance - Compliance to all relevant nations' Legal requirements including Data Protection Act (1998) Freedom of Information Act (2001) & Privacy laws.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Granicus will comply with its obligations under the UK Data Protection Act of 1998 and other applicable data privacy laws and regulations. In addition, we are fully aware of the upcoming GDPR legislation coming into force in May 2018 and are committed to full compliance.

77. Data purging/archiving - There should be an option/routine to purge/archive data in accordance with an agreed data retention policy.

The GovDelivery Communications Cloud service is fully compliant with this objective.

Granicus will keep a complete archive of GovDelivery Communications Cloud data created by CQC, including message sends and subscriber history for 18 months (rolling). Additionally, full back ups are retained for one year and then destroyed.

Support

78. Service desk & service manager - Supplier shall provide a Service Desk with ability to log and resolve incidents and requests. Supplier shall provide a named contact for escalation of issues and regular interface between the supplier and the customer.

The GovDelivery Communications Cloud service is fully compliant with this objective. Ongoing

support is provided throughout the length of the contract.

CQC will have a named Account Manager to help maximise the use of the GovDelivery service, in addition to being the regular interface between the supplier and the customer and as the initial point of contact for any escalation of issues.

Granicus agrees to provide CQC with complete technical support. Regular support will be available during regular business hours. Monday-Friday; via email or Freephone telephone call, covering all issues. Emergency support will be available 24x7; via Freephone telephone call.

Emergency issues include only those issues that are preventing effective use of the system; other issues must be addressed during business hours. Use-based questions should be directed to CQC's Account Manager, who will escalate questions to experienced technical personnel as necessary. Technical personnel include a team of

dedicated Cloud Engineers and support consultants. CQC will have after- hours access to Granicus customer service.

The Granicus Customer Support Team manages technical requests and issues through a ticketing system via phone, email, or online at support.govdelivery.com the hours: 9:00 AM to 10:00 PM. In addition, 24-hour emergency phone support is available during off-business hours. All customer support requests are covered under the subscription.

Granicus also agrees to provide CQC with complete help-desk support for administrators and end-users (optional, but at no charge). Regular support will be available during regular business hours, Monday- Friday; via email or Freephone telephone, covering all issues. The first step in fielding a general support or maintenance issue is with the account manager who will escalate issues to technical personnel as necessary. CQC can contact the account manager by email or phone and CQC can allow end-users to contact the account manager directly by email.

Accessibility

79. Accessibility – The system shall enable accessibility via assistive technology for those who cannot use a standard mouse and/or keyboard e.g. WA3, Dragon Speak and Windows 7 Voice Recognition software.

The GovDelivery Communications Cloud service is fully compliant with this objective.

The Communications Cloud is Section 508 compliant (US accessibility standard) and has been tested to WA3 level by UK clients including the RNIB who have used the service.

3. Service Levels & Volumes

GovDelivery Communications Cloud is a SaaS (Software as a Service) cloud delivery application which maintains and offers the highest standards. With the service being used by over 1,800 government organisations globally, we maintain a robust and highly scalable platform which can flex and cope with huge volumes.

Granicus has no hesitation in recommending continued usage of our service, and foresee no issues at all with being able to deliver a high quality and reliable service to CQC.

Through the GovDelivery Communications Cloud, over 11 billion messages on behalf of government globally. For reference HMRC have been a long-standing user of GovDelivery and frequently use the service with sends of up to 20 million emails per month.

We successfully processed over 3.2M messages for CQC during the last 12 months, and based on the above, we have no concerns in being able to maintain and exceed the current service levels.

4. Cost Envelope

Cost Envelope
£100,000 up to £120,000 including VAT

Granicus are pleased to offer CQC pricing options that fit within this pricing range. As instructed, we have fully detailed all pricing options and further details within the Commercial Response document submitted as part of this tender response.

5. Length of Contract

Start Date	End Date	Extension (If Applicable)
30th January 2018	29th January 2020	29th January 2021 (G-Cloud 9 extended term)

Granicus is a G-Cloud listed supplier and as such offers great flexibility with contracts. CQC are familiar with procuring on G-Cloud as per the current –Cloud contract for GovDelivery Communications Cloud.

The initial maximum term permissible with G-Cloud is 24 months, however CQC have the option to further extend the contract at the end of this period, for a further 12 months.

The extended period would allow CQC to benefit from another years' service under the current G-Cloud 9 pricing, keeping the cost fixed and allowing CQC to budget effectively.

Procuring via G-Cloud comes with the benefit of allowing CQC to terminate the GovDelivery Communications Cloud service at any time (with 30 days' notice) and/or make changes to the licence, without penalty.

6. Timetable for procurement exercise

The table below sets out the summary timetable for this procurement exercise. Please note that this timetable is intended as a guide, and whilst CQC does not intend to depart from the timetable, it reserves the right to do so at any time. In the event that there any changes to the timetable become necessary, CQC will notify all participating Tenderers of any such changes.

Activity	Date
Invitation to participate in further competition process issued	15/12/2017
Deadline for receipt of clarification questions from Tenderers	04/01/2018
Tender submission deadline	12/01/2018
Initial evaluation and moderation of Tender submissions	16/01/2018
Contract award (anticipated)	18/01/2018
Contract implementation (anticipated)	29/01/2018

Granicus has noted this timetable and has no concerns in working within the timeframes quoted.

7. Authority Responsibilities

The supplier will appoint a contract manager who will oversee the work and liaise with the CQC contract manager. Both contract managers will arrange quality meetings as above.

A Granicus Account Manager will liaise with CQC to ensure that any work required to deliver the service, providing any changes are made, are done in a timely fashion. Being a live service, should no changes be made to the existing licence, there will be no need to conduct any setup work.

The Granicus Account Manager will facilitate any meetings between CQC and our in-house Implementation team to cover all activities required to change/amend the scope of the service.

Granicus offers a range of options for quality meetings, whether in-person, teleconference, or online web meetings. Typically, administrator training is delivered online, allowing for easy recording and playback for future use within CQC.

8. Contractor Responsibilities

CQC will expect the supplier to fully cooperate in the exit strategy of the service at its contract end. This will include formulating a transition plan, possible parallel working and active cooperation with CQC and the incoming supplier. The outgoing supplier will get a plan 6 months before the contract end date, with allowance for a 3-month exit period.

Granicus will fully cooperate with this exit strategy and work with CQC and any incoming supplier/s to ensure that any transition is as smooth as possible, with little or no disruption to any live service.

Should CQC decide to cancel the service, Granicus will work closely with CQC to ensure a smooth cessation of service. We will actively work with CQC staff to formulate a viable transition plan and cooperate and work with any new incoming supplier to transition the service

9. Contract Management Arrangement

Regular meetings to be put in place.

Granicus are happy to meet with CQC with regards to any aspect of this contract, in addition to scheduling regular service review/progress meetings.

With an Account Manager and Client Success Consultant assigned to work with CQC, Granicus will always be on hand and available to discuss anything service related.

Being a subscription service, it is in our interest to ensure that customers realise success and get the most value from the platform. Granicus will schedule regular meetings with CQC to share best practices across government, monitor account growth, and introduce new features and offer training where needed to help the organisation realise value and achieve measurable outcomes.

10. Key Performance Indicators

As outlined in earlier sections, the GovDelivery Communications Cloud service has historically enjoyed market leading uptime and availability. Working with all levels of government worldwide, system availability and security comes top of our executive priorities.

For the entire year of 2017, Communications Cloud gained service availability of 99.9%, Monday to Sunday. The GovDelivery service is fully compliant with CQC's desired service availability levels.

Indicator	Measured by	Reference Point or Target	Review Date
Any system is required to meet service availability levels of 99.5% Monday to Friday. 5 days a week with the exception of UK bank holidays	*The GovDelivery Communications Cloud service availability is routinely measured by the Uptime Institute (external company).*	*Granicus will strive to maintain uptime availability levels of 99.9%, however will notify CQC if levels drop below 99.5%*	*Reviewed 2-weekly*
System Maintenance outside working hours	*GovDelivery Technical Operations*	*Granicus will strive to provide system maintenance and releases outside normal business hours as much as possible. The 99.9% service availability figure includes planned system maintenance.*	*Reviewed 2-weekly*

11. Service Credits (if applicable)

Granicus do not offer a financial recompense model for not meeting service levels, and we do not have a lock-in period or impose any termination charges.

12. Milestones

Continuing with the existing GovDelivery Communications Cloud solution would require no implementation effort or cost. The service can continue to be used as is now and CQC can assume business as usual from 30th January 2018.

Should CQC upgrade to the GovDelivery Professional Communications Cloud Licence, there will be no impact or disruption to the existing functionality and admins can continue using the system as they do now, however, the additional functionality and features will become available within the account and GovDelivery will have a dedicated Implementation consultant assigned to CQC to work on any configuration and training required.

The details in the table below all relate to, and are on the basis of, CQC upgrading their licence to the Professional licence:

Description	Target Date	Action to Achieve Milestone	Review Date
Kick – off meeting	N/A - service is stood up	N/A - service is stood up	N/A - service is stood up
System build / Activation of Professional Licence (if required)	w/c 29th January 2018	Granicus to activate licence.	w/c 5th February 2018
Training (if required)	w/c 5th February	Granicus will assign a named Implementation Consultant to the project who will reach out to CQC.	w/c 19th February 2018
Testing (if required)	By w/c 29th February 2018	Granicus and CQC to meet and discuss testing.	28th February 2018
Website integration (if required)	N/A	N/A	N/A
Launch- by end of January	Service will be live	Service will be live	Service will be live
Initial evaluation meeting – by end of March	w/c 12th March 2018	Granicus and CQC to meet to discuss progress/advanced usage	30th March 2018

13. Skills and Knowledge Transfer

CQC seeks to ensure that the chosen supplier will transfer knowledge back into the Authority and exit the contract in such a way as to facilitate re-procurement and/or project termination.

The GovDelivery Communications Cloud service is a Software as a Service (SaaS). As such there is no equipment held on the CQC site so there is no requirement for a decommissioning plan.

Should CQC decide to cancel the service, Granicus will work closely with CQC to ensure a smooth cessation of service.

We will agree a date with CQC on which to cease the service and not send any messages or capture any new sign ups.

Granicus would remove CQC from the network sign up options list.

CQC would need to remove any sign up overlay or snippets from their website and the Granicus support team can provide guidance on this.

All of the subscriber data uploaded to the GovDelivery Communications Cloud and contained within the GovDelivery account, including from CQC via the CQC website sign ups or initial databases, will be returned to CQC in a CSV file format. This includes all subscriber email addresses, subscriber metadata and topics/categories within the account.

The off-boarding process is designed to be seamless and requires little effort from CQC should they wish to terminate. Data dumps are structured in such a way that should CQC opt to procure another service and migrate data, or terminate the project, Granicus will make the format and process as easy as possible for CQC.

Throughout the life of the contract, CQC will have access to a wide range of best practice guides, webinars, and a Success Consultant on hand to work with the CQC team, sharing industry knowledge and examples of success across a wide range of central and local government organisations who use the GovDelivery platform. All of these skills, and knowledge acquired throughout the contract would be retained by CQC staff to apply to any future digital communications tools or applications.

Schedule 2 - Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

Basic (existing) Licence

Minimum initial term: 12 months
Maximum initial term: 24 months
Terms and Conditions of sale: G-Cloud 9
Based on the existing figure of 1,000,000 unique website visitors per quarter
Monthly service fee: £2,815 + vat / £3,378 including vat.
Setup: N/A in this case as CQC are already enjoying the benefit of the live service
Total 12 month fee: £33,780 + vat / £40,536 incl. vat
Total 24 month fee: £67,560 + vat / £81,072 incl. vat

Part B - Terms and conditions

1. Call-Off Contract start date and length

1.1   The Supplier must start providing the Services on the date specified in the Order Form.

1.2   This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3   The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4   The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

2.1   The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the

Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.62 (Data protection and disclosure)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2   The Framework Agreement provisions in clause 2.1 will be modified as follows:

- a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

- a reference to 'CCS' will be a reference to 'the Buyer'

- a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3   The Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', where 'XX' is the Framework Agreement clause number.

2.4   When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1   The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2   The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1   The Supplier Staff must:
- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- complete any necessary Supplier Staff vetting as specified by the Buyer

4.2   The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3   The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4   The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5   The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.

4.6   The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and

promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
- are confident that they can fulfil their obligations according to the Call-Off Contract terms
- have raised all due diligence questions before signing the Call-Off Contract
- have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and

must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2   The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3   If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4   If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

- a broker's verification of insurance

- receipts for the insurance premium

- evidence of payment of the latest premiums due

9.5   Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any insurances
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6   The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7   The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are

due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

- premiums, which it will pay promptly

- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Act (DPA) or under incorporated Framework Agreement clauses 8.83 to 8.91. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

- rights granted to the Buyer under this Call-Off Contract

- Supplier's performance of the Services

- use by the Buyer of the Services

11.6   If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

- modify the relevant part of the Services without reducing its functionality or performance

- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.7   Clause 11.5 will not apply if the IPR Claim is from:

- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

- other material provided by the Buyer necessary for the Services

11.8   If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of Information

12.1   The Supplier must:

- comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

- only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

- take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2   The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

- providing the Buyer with full details of the complaint or request

- complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the

timescales required by the Buyer)

- providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

The Supplier must not remove any proprietary notices in the Buyer Data.

13.1 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policy and all Buyer requirements in the Order Form.

13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications

- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets

- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection

- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

- the security requirements of cloud services using the NCSC Cloud Security Principles and

accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6   The Buyer will specify any security requirements for this project in the Order Form.

13.7   If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.8   The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.9   The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1   The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2   The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

14.3   If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4   If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5   The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1   All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2   If software needs to be converted before publication as open source, the Supplier must also provide the

converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

● Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

● Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

17. Guarantee

17.1   If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start Date:

- an executed Guarantee in the form at Schedule 5

- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1   The Buyer can End this Call-Off Contract at any time by giving the notice to the Supplier specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2   The Parties agree that the:

- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

- Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

18.3   Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4   The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

- any fraud

18.5   A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

- an Insolvency Event of the other Party happens

- the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

- any rights, remedies or obligations accrued before its Ending or expiration

- the right of either Party to recover any amount outstanding at the time of Ending or expiry

- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)

- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

- work with the Buyer on any ongoing work

- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

Manner of delivery	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line

with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3   If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

21.4   The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5   Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6   The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

● the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer

● there will be no adverse impact on service continuity

● there is no vendor lock-in to the Supplier's Service at exit

● it enables the Buyer to meet its obligations under the Technology Code Of Practice

21.7   If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8   The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

● the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

● the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

● the transfer of Project Specific IPR items and other Buyer customisations, configurations and

databases to the Buyer or a replacement supplier

- the testing and assurance strategy for exported Buyer Data

- if relevant, TUPE-related activity to comply with the TUPE regulations

- any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

- other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more

than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure,

assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form

- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

25.1   If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2   The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3   The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4   This clause does not create a tenancy or exclusive right of occupation.

25.5   While on the Buyer's premises, the Supplier will:

- comply with any security requirements at the premises and not do anything to weaken the security of the premises

- comply with Buyer requirements for the conduct of personnel

- comply with any health and safety measures implemented by the Buyer

- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6   The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1   The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2   Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no

liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start Date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- the activities they perform

- age

- start date

- place of work

- notice period

- redundancy payment entitlement

- salary, benefits and pension entitlements

- employment status

- identity of employer

- working arrangements

- outstanding liabilities

- sickness absence

- copies of all relevant employment contracts and related documents

- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

29.3   The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4   In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5   The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6   The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

- its failure to comply with the provisions of this clause

- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.7   The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8   For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1   The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2   If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1   If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start Date in the form set out in Schedule 3.

31.2   In addition to any obligations under the Collaboration Agreement, the Supplier must:

- work proactively and in good faith with each of the Buyer's contractors

- co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1   The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2   The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3   If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

Schedule 3 - Collaboration agreement

The Collaboration agreement is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 4 - Alternative clauses

The Alternative clauses are available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 5 - Guarantee

The Guarantee is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.

Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: - information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above - other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Crown	The government of the United Kingdom (including the Northern Ireland

	Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Protection Legislation or DPA	The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.
Data Subject	Will have the same meaning as set out in the Data Protection Act 1998.
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.

Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557ix together with the

	Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be:

	● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the

	meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and **'Losses'** will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a

	Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	As described in the Data Protection Act 1998 (http://www.legislation.gov.uk/ukpga/1998/29/contents)
Processing	This has the meaning given to it under the Data Protection Act 1998 as amended but, for the purposes of this Call-Off Contract, it will include both manual and automatic processing. 'Process' and 'processed' will be interpreted accordingly.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: - induce that person to perform improperly a relevant function or activity - reward that person for improper performance of a relevant function or activity - commit any offence: - under the Bribery Act 2010 - under legislation creating offences concerning Fraud - at common Law concerning Fraud - committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute,

	codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and

	services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.