



Crown
Commercial
Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	25
Schedule 1: Services	46
Schedule 2: Call-Off Contract charges	48
Schedule 6: Glossary and interpretations	51
Schedule 7: UK GDPR Information	66
Annex 1: Processing Personal Data	65
Schedule 8: Cabinet Office T&S Policy	69
Annex 3: Social Value	72

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	680677614553449
Call-Off Contract reference	WP2131
Call-Off Contract title	WP2131 - SMS Provider for GOV.UK Notify
Call-Off Contract description	GOV.UK Notify is a multi-channel digital communications platform that UK public sector service teams can use to send emails, text messages, and letters to users of their service. These messages will typically be status updates, requests for action, receipts of applications or supporting information, and reminders
Start date	01 April 2023
Expiry date	31 March 2024 (+12 month extension option with pricing review on 02 January 2024)
Call-Off Contract value	Up to £38,681,500 (exc. VAT) (includes 12 months extension)
Charging method	BACS Monthly in arrears
Purchase order number	To follow

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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 Services 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	Buyer's name: Government Digital Service (GDS), Cabinet Office Buyer's email: commissioning-digital@digital.cabinet-office.gov.uk Buyer's main address: Cabinet Office, 1 Horse Guards Road, London, SW1A 2HQ. GDS: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS
To the Supplier	Supplier's Name: FireText Communications Limited Supplier's Address: [REDACTED] [REDACTED] [REDACTED] Company number: [REDACTED]
Together the 'Parties'	

Principal contact details

For the Buyer:

Job Title: Delivery Manager

Name: [REDACTED] [REDACTED]

Email: [REDACTED].[REDACTED]@[REDACTED].[REDACTED]-[REDACTED].[REDACTED].[REDACTED]

Phone: [REDACTED] [REDACTED]

For the Supplier

Job Title: Account Manager

Name: [REDACTED] [REDACTED]

Email: [REDACTED].[REDACTED].[REDACTED].[REDACTED].[REDACTED]

Phone: [REDACTED] [REDACTED] [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 01 April 2023 and is valid for 12 months .
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least [90] Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of [30] days from the date of written notice for Ending without cause (as per clause 18.1).</p>
Extension period	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 1 months written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>The contract extension will be subject to pricing review to be undertaken on 02 January 2024 or at the earliest opportunity thereafter.</p>

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	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none">• Lot 2: Cloud software
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <ul style="list-style-type: none">• Service ID; 680677614553449• Service Description; FireText Communications Limited FireText UK Secure (Official) SMS, RCS, WhatsApp and Advanced Messaging <p>Link to Service Description; https://redirect.contractawardservice.crowncommercial.gov.uk/g-clou</p>

	<p>d/services?id=680677614553449</p> <p>There is no guarantee to the Supplier of volume of Services required and the Buyer may increase or decrease the volume of Services to meet its flexible requirements.</p>
Additional Services	Not used
Location	<p>The Services will be delivered online through an Application Programming Interface.</p> <p>The Buyer will require access to the service from The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS.</p>
Quality Standards	<p>The quality standards required for this Call-Off Contract are:</p> <ul style="list-style-type: none"> • Provide a data retention policy to the agreed levels at contract commencement and inform the Buyer of any changes to the policy, including for all Supplier subprocessors • Guaranteed delivery to the network times where 99.95% of all messages are delivered to the Mobile Network Operators within 10 seconds • Reporting, to include: <ul style="list-style-type: none"> • delivery status within 72 hours or as soon as a status is available with a retry of minimum 3 hours • international SMS delivery rates and sender IDs • Approach to multi-tenancy and prioritisation, which is shared with the Buyer before contract commences for approval - any failover site should not be used to handle more than 1% of production traffic except at any given time, except in case of an incident; ability to automatically scale for traffic increase up to the total required notifications per second without any prior notice
Technical Standards:	<p>The technical standards required for this Call-Off Contract are:</p> <ul style="list-style-type: none"> • Data location (also see Security Requirements 1, 12,13, 14 and 15 below) • REST API • JSON data exchange format • Rate limiting • HTTPS/SSL (also see Security Requirements 26 and 27 below) <p>The Government Technology Code of Practice https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice</p> <p>The Government Service Standard (where applicable) https://www.gov.uk/service-manual/service-standard</p>

	<p>The Minimum Cyber Security Standard https://www.gov.uk/government/publications/the-minimum-cyber-security-standard</p> <p>The Government Cyber Security Policy Framework (publication expected in April 2023)</p>
Security Standards & Requirements	<p>The Security Standards and Requirements for this Call-Off Contract are those specified in the Terms and Conditions 13.6 and 16, plus:</p> <ol style="list-style-type: none"> 1) The Supplier and entities in its supply chain, shall not be: <ol style="list-style-type: none"> a) an entity constituted or organised under the law of Russia or Belarus; or b) an entity registered in the UK or with substantive business operations in the UK, or another country but controlled by an entity based in Russia or Belarus e.g. a parent company or by 'Persons of Significant Control' as described in Procurement Policy Note 01/22, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/526200/ppn_update_cyber_essentials_0914.pdf 2) The Supplier shall not be an Affiliate of any other entity providing similar services to the Buyer. 3) When providing the Services, the Supplier shall not use an SMS aggregator that is also being used by other entities providing similar services to the Buyer. 4) The Supplier (and any SMS aggregators it uses) shall not share any infrastructure used for the delivery of the Services with any other entity providing similar services to the Buyer. 5) The Supplier and any SMS aggregators used shall be an active participant in the MEF Registry, https://mobileecosystemforum.com/sms-senderid-protection-registry/ and be awarded the 'Trust in Enterprise Messaging' badge. 6) The Supplier shall sign up and adhere to the A2P Code of Conduct, https://mobileecosystemforum.com/programmes/future%20-of-messaging/fraud-management/trust-in-enterprise%20messaging/ 7) The Supplier shall disclose to the Buyer how they route messaging traffic on a destination network by destination

network basis.

- 8) The Supplier shall have back-to-back contracts along the length of the SMS delivery chain to ensure that the described SMS delivery route is authorised, legal and all relevant parties are accountable.
- 9) The Supplier shall ensure that the information security of the Services, including any elements provided by subcontractors, is managed using an Information Security Management System that is certified by a UKAS-accredited auditor as meeting the ISO/IEC 27001:2013 standard (or a successor standard).
- 10) The Supplier shall ensure that the Buyer's security and assurance requirements are flowed down to and are implemented by all relevant subcontractors in its supply chain.
- 11) The Supplier shall ensure that its staff and subcontractor staff are appropriately trained and made aware of their obligations to secure and protect Notify Data.
- 12) The Supplier shall use dedicated hardware and software to provide the Services which is not shared with other service providers and is hosted on infrastructure and data centres physically located in the UK. Note: this includes both production and any fail-over instances. The Supplier must obtain the Buyer's authorisation before making any changes to this arrangement.
- 13) The Supplier shall ensure that all Supplier staff, including subcontractors, with access to the Services or the ability to otherwise affect the Services are located in the UK and have successfully completed pre-employment screening that, as a minimum, includes:
 - a) verification of identity
 - b) verification of immigration status
 - c) verification of employment history
 - d) a DBS criminal records check for unspent convictions.

Note: screening conducted in accordance with BS7858:2019 would satisfy this requirement.

- 14) The Supplier shall ensure that Notify Data is only processed and stored within the EEA.
- 15) The Supplier shall ensure that all support and administration of the Services, (including SMS aggregator services if used), is provided by staff located in the UK

unless otherwise agreed with the Buyer.

- 16) The Supplier shall provide the Buyer with details of the supply chain providing the Services (including infrastructure service providers, data centres providers and SMS aggregators), and shall notify the Buyer in advance of making any changes to this.
- 17) The Supplier shall provide direct connections between its SMS platform and the UK mobile network operators; any use of SMS aggregators shall require the prior approval of the Buyer and the aggregator must provide direct connections between its platform and the mobile network operators.
- 18) Where the Services are multi-tenanted, the Supplier shall ensure that effective logical or physical controls are implemented throughout the SMS delivery chain to maintain separation between Notify Data and other customers.
- 19) The Supplier shall ensure that potentially service-affecting support requests are only accepted from authorised representatives of the Buyer by implementing procedural and technical controls to provide strong authentication of individuals raising such requests; these controls shall be agreed with the Buyer.
- 20) The Supplier shall ensure that all end-user devices, IT systems and network equipment used by the Supplier (and its subcontractors) to deliver the Services are within the scope of a current certification (see <https://www.ncsc.gov.uk/cyberessentials/overview>) and include appropriate measures to minimise the risk of malware execution.
- 21) The Supplier shall ensure that administrative interfaces to the Services used by the Supplier's (and its subcontractors') operations and support staff utilise multi-factor authentication.
- 22) The Supplier shall ensure that management console interfaces to the Services used by the Buyer support the use of multi-factor authentication.
- 23) The Supplier (and subcontractors) shall take active measures to defend interfaces to the Services against authentication attacks, like password sprays and common weak passwords.
- 24) The Supplier shall ensure that API interfaces to the Services used by the Buyer authenticate API requests so that the Supplier can be confident of the requestor's

identity.

25) The Supplier shall ensure that API interfaces to the Services used by the Buyer enable the Buyer to verify the identity of the interface by presenting a digital certificate signed by a reputable certificate authority.

26) Unless otherwise agreed with the Buyer, the Supplier shall ensure that the Services, including any elements provided by subcontractors, protect all Notify Data whilst in transit using either TLS or an IPsec VPN. This includes data in transit:

- a) between the Buyer's end-user devices and the Services' web interfaces
- b) between the Buyer's applications and the Services' APIs
- c) internally within the Services
- d) between the Supplier's SMS platform and the mobile network operators' networks, or
- e) between the Supplier's SMS platform and any subcontractors (e.g SMS aggregators) used
- f) between any subcontractors (e.g. SMS aggregators) and the mobile network operators' networks

27) Unless otherwise agreed with the Buyer, TLS and IPsec VPN implementations used by the Services shall be aligned with the latest NCSC guidance, currently published at:

- <https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data>
- <https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data>

TLS endpoints used to provide the Services must enable clients to negotiate connections that utilise TLS V1.2 (or above) and a cipher suite recommended by the NCSC. TLS endpoints shall not support vulnerable versions of TLS and vulnerable cipher suites.

28) The Supplier shall protect Notify Data from unauthorised access, through the use of appropriate physical controls (such as purpose-built data centres with multi-layered physical access controls, intruder alarm systems, trained security guards on duty 24x7, CCTV). The Supplier shall ensure that Data centres where Notify Data is processed

have been certified against a recognised and appropriate standard that covers physical security - appropriate standards include CSA CCM v3.0.1 and ISAE 3402.

- 29) The Supplier shall ensure that all Notify Data, including any metadata and logs derived from that data, is encrypted at rest in order to protect it from unauthorised access by parties with physical access to infrastructure. This can be achieved using full-disk encryption, application-layer encryption, or both. A symmetric encryption algorithm shall be used in a mode of operation that provides both confidentiality (to prevent unauthorised reading of the data) and integrity (to prevent un-noticed tampering of the encrypted data). Both the algorithm and mode of operation used should be approved for general use, for example, an algorithm from NIST-SP-800-131A, and a suitable mode of operation from NIST-SP-800-38. (At the time of writing, these include the symmetric algorithm AES, and the modes of operation GCM and XTS, sometimes described as 'AES-GCM' or 'AES-XTS'). The Supplier shall ensure that data encrypting keys and key encrypting keys are protected through their full lifecycle.
- 30) The Supplier shall track all equipment containing Notify Data and ensure that any components containing Notify Data are sanitised in accordance with the latest NCSC guidance currently published at <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media> when components are removed for repair, replaced, reused or reach end of life.
- 31) The Supplier shall ensure that robust key disposal mechanisms, such as FIPS 140-2 HSMs, are used within the delivery chain.
- 32) The Supplier shall erase Notify Data when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.
- 33) The Supplier shall ensure that redundant accounts and credentials are revoked at the earliest opportunity.
- 34) The Supplier shall collect event logs pertaining to the use of and access to the Services and the infrastructure hosting the Services. The Supplier shall retain the event logs for a period of six months (unless otherwise agreed with the Buyer) and the Supplier shall make the event logs available to the Buyer on request.
- 35) The Supplier shall log and audit all accesses made to production systems and the Notify Data hosted on them; an administrator accessing Notify Data or making changes

	<p>that affect the Buyer's use of the service shall be reliably logged and monitored.</p> <p>36) The Supplier (and subcontractors) shall employ technical and procedural controls to reduce the likelihood of accidental or malicious compromise by its staff.</p> <p>37) The Supplier must ensure that all privileged access to production systems occurs from corporately-management end-user devices that are dedicated to management functions.</p> <p>38) The Supplier shall ensure that the Services are protectively monitored to enable the Supplier and subcontractors to detect and respond quickly to security incidents such as unauthorised access to and misuse of the Services.</p> <p>39) The Supplier shall ensure that all software used by the Services is supported by a vendor or active project such that security patches for newly-discovered vulnerabilities will be made available.</p> <p>40) The Supplier shall ensure that it (or any relevant subcontractor) applies security patches to software vulnerabilities in the Services no later than:</p> <ul style="list-style-type: none"> a) seven (7) days after the public release of patches for vulnerabilities classified as "critical"; b) thirty (30) days after the public release of patches for vulnerabilities classified as "important"; and c) sixty (60) days after the public release of patches for vulnerabilities classified as "other" <p>41) The Supplier shall ensure that vulnerabilities identified in the SMS delivery chain are tracked until mitigations have been deployed using a suitable change management process.</p> <p>42) The Supplier shall maintain a list of external software dependencies in the SMS delivery chain, shall have a vulnerability management process that includes identifying and remediating issues in these. On request the Supplier shall make the list available to the Buyer.</p> <p>43) The Supplier (and any subcontractors it uses) shall have a process for considering the severity and impact of threats and vulnerabilities within the context of the Services and for prioritising the implementation of mitigations.</p> <p>44) The Supplier shall arrange, at its cost, for independent IT Health Checks of the infrastructure and systems that provide the Services to take place at least annually, and</p>
--	--

after significant changes. The scope of the IT Health Checks shall include:

- a) Testing applications for common vulnerabilities such as those described in the OWASP ASVS (see <https://owasp.org/www-project-application-security-verification-standard>)
- b) Reviewing the configuration of infrastructure, software versions and patch levels
- c) Testing the effectiveness of access controls, including administration interfaces used by the Supplier (and its subcontractors) to administer the Services and infrastructure
- d) Testing the effectiveness of controls providing separation between customers
- e) Testing the configuration and effectiveness of data in transit and data at rest protection.

IT Health Checks shall be conducted by a 'Green Light' CHECK company, as listed on the NCSC's website, or teams qualified under one of these certifications schemes: CREST, Tiger Scheme, Cyber Scheme. Where the Supplier uses subcontractors, equivalent IT Health Checks are required of the relevant infrastructure and systems.

- 45) The Supplier shall have pre-defined processes in place for responding to common types of cyber security incidents and attacks and shall ensure that these processes are actively deployed in response to such incidents.
- 46) The Supplier shall report any Security Incident to the Buyer without undue delay, and where possible no later than 6 hours after the event is discovered. Security Incidents should be reported to the points of contact as agreed with the Buyer.
- 47) The Supplier shall ensure that public-facing interfaces to the Services have effective measures in place to mitigate against DDoS attacks.
- 48) The Supplier shall provide a test environment, representative of the Services, which the Buyer can use, without charge, to conduct smoke tests of the integration between Notify and the Services without sending real messages.
- 49) The Supplier must ensure that secure software development practices are followed by the Supplier and subcontractors when developing software for the Services:

	<ul style="list-style-type: none"> a) Where software is developed, a software development lifecycle must be followed that is aligned with secure software development and deployment guidance. b) Developers shall be trained in secure development c) Security must be considered throughout the design and development process d) Well-understood libraries shall be used for security-critical functions e) Separate production, testing and development environments shall be used f) Developers shall be able to trace all deployed software back to the source code that produced it. <p>50) The Supplier must be able to support the use of at least two API keys at the same time for the Buyer to authenticate with the Supplier's API to enable zero downtime credential rotation.</p> <p>51) The Supplier shall make available any assurance materials reasonably requested by the Buyer in order to demonstrate that the Supplier and its subcontractors are meeting the Buyer's security and assurance requirements, including:</p> <ul style="list-style-type: none"> a) A list of subcontractors used by the Supplier (to be provided prior to contract commencement and whenever changes occur). b) Details of the SMS delivery chain and SMS routes used, including how the Supplier routes messaging traffic on a destination network by destination network basis (to be provided prior to contract commencement and whenever changes occur). c) Evidence that the Supplier has back-to-back contracts in place covering the length of the SMS delivery chain (prior to contract commencement and whenever changes occur). d) Evidence (e.g. a letter) from each connected MNO confirming that a direct connection is in place between the Supplier and the MNO (to be provided prior to contract commencement and whenever changes occur). e) Cyber Essentials Plus certificates (to be provided prior to contract commencement and annually thereafter).
--	--

	<p>f) ISO/IEC 27001 certificates and scope descriptions (to be provided prior to contract commencement and annually thereafter).</p> <p>g) Evidence that data centres where Notify Data is processed have been certified against a recognised and appropriate standard that covers physical security (to be provided prior to contract commencement and annually thereafter).</p> <p>h) Evidence that IT Health Checks covering the scope described in Security Requirement 44 are taking place (to be provided prior to contract commencement and at least annually thereafter).</p> <p>i) Evidence that the personnel security requirements described in Security Requirement 13 are being met (to be provided prior to contract commencement and annually thereafter).</p> <p>j) Security policies, standards and procedures.</p>
Service level agreement:	<p>The service level and availability criteria required for this Call-Off Contract are:</p> <ul style="list-style-type: none"> ● HTTP API uptime 24/7/365 of 99.95% as measured on a monthly basis. If the supplier's performance is deemed 'inadequate' for more than 1 month, this will constitute critical service failure (see KPIs for information on criteria) ● 99.95% of all text messages are sent to the Mobile Network Operators within 10 seconds. If the supplier's performance is deemed 'inadequate' for more than 1 month, this will constitute critical service failure (see KPIs for information on criteria) <ul style="list-style-type: none"> ○ As part of the RFC, Firetext were asked to confirm "(d) Message sending rate of 1000/s or above for 6 fragment messages" <ul style="list-style-type: none"> ■ Firetext' response - "Yes" ● P1 support response times in line within definitions in the Key Performance indicators. If the supplier's performance is deemed 'inadequate' for more than 1 month, this will constitute critical service failure (see KPIs for information on criteria) ● Percentage of messages delivered and failed <ul style="list-style-type: none"> ● Minimum 90% successfully delivered ● Maximum 10% temporary failure ● Maximum 10% permanent failure ● The Supplier will replay delivery receipts for 3 days. <p>If the supplier has a critical service failure, remedial actions should be presented in writing and agreed with the Buyer within 2 working days</p>

	of identifying the critical service level failure. If these are not satisfactory, as deemed by the Buyer, or if the supplier has more than one critical service level failure for the duration of the contract, the Buyer can terminate the contract within the contractual notice period.
Onboarding	The supplier shall provide a written up-to-date Business Continuity and Disaster Recovery (BCDR) Plan within 1 month of signing the contract . This should be formally accepted when completed to the satisfaction of the Buyer.
Offboarding	<p>The supplier shall provide a written Exit Plan within 2 months of signing the contract.</p> <p>The Supplier will work with the Buyer and provide the Off-Boarding Requirements/Services, as part of the Exit Plan, including:</p> <ul style="list-style-type: none"> • technical work to disconnect from Buyer's infrastructure • data return and destruction within agreed timescales at agreed service levels • enabling any short codes and virtual mobile numbers used by the Buyer to be ported to another SMS service provider. The process for porting both short codes and virtual mobile numbers should be detailed in the Exit Plan and should be at no additional cost to the Buyer. <p>The Exit Plan for this Call-Off Contract should also reference offboarding details in the Service Description and Service Definition.</p> <p>The Exit Plans should be formally accepted when completed to the satisfaction of the Buyer.</p>

Collaboration agreement	Not used
--------------------------------	----------

Limit on Parties' liability	<p>The annual total liability of either Party for all Property defaults will not exceed £1,000,000.</p> <p>The annual total liability for Buyer Data defaults will not exceed £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability for all other defaults will not exceed the greater of £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
Insurance	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> • 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 • Cyber and Data Protection Insurance
Buyer's responsibilities	<p>Not used</p>
Buyer's equipment	<p>Not used</p>

Supplier's information

Subcontractors or partners	<p>The following is a list of the Supplier's Subcontractors or Partners used to deliver the Services:</p> <p>[REDACTED]</p> <p>Message Delivery Partners:</p> <p>[REDACTED]</p>
-----------------------------------	---

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	<p>The payment method for this Call-Off Contract is: Monthly in arrears to: Bank: [REDACTED] Sort Code: [REDACTED] Account: [REDACTED]</p>
Payment profile	<p>The payment profile for this Call-Off Contract is monthly in arrears by BACS.</p> <p>There is no guarantee to the Supplier of volume and volumes may flex up or down to complete the requirements. GDS reserves the right to allocate work between suppliers at its absolute discretion</p>
Invoice details	<p>The Supplier will issue valid electronic invoices monthly in arrears. The Buyer will pay the Supplier within thirty (30) days of receipt of a valid invoice..</p>
Who and where to send invoices to	<p>Invoices will be sent to: xxxxx.xxxxxxx@xxxxxxx.cabinet-office.gov.uk and also to APinvoices-CAB-U@gov.sscl.com, which is at Cabinet Office, PO Box</p>

	405, SSCL, Phoenix House, Celtic Springs Business Park, Newport, NP10 8FZ.
Invoice information required	<p>All invoices must include the WP number and Purchase Order Number.</p> <p>Each invoice shall be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges and total charge for the invoice period, in sufficient detail to enable the Customer to validate the invoice.</p>
Invoice frequency	Invoice will be sent to the Buyer Monthly in arrears
Call-Off Contract value	<p>The total value of this Call-Off Contract is Up to £38,681,500 (exc. VAT)</p> <p>Includes optional 12 month extension (pricing to be reviewed 02/01/2024)</p>
Call-Off Contract charges	The breakdown of the Charges is shown in Schedule 2

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following milestones:</p> <ul style="list-style-type: none"> • Provision of approach to multi-tenancy and prioritisation - to be shared and agreed with Buyer before contract commences (refer to Quality Standards). • Provision of a data retention policy before the contract commences (refer to Quality Standards).
-----------------------------------	---

	<ul style="list-style-type: none"> • Provision of SMS services - from day 1 of contract commencement • Access to live dashboard for reporting - from day 1 of contract commencement • Provision of written BCDR plan within 1 month of contract commencement • Provision of written Exit plan within 2 months of contract commencement • Implementation of Exit and Offboarding plan - no later than 1 month before contract end
Guarantee	Not used
Warranties, representations	In addition to the incorporated Framework Agreement clause 2.3, the Supplier warrants and represents to the Buyer that there are no additional warranties and representations].
Supplemental requirements in addition to the Call-Off terms	<p>Key Performance Indicators (KPIs)</p> <p>The KPIs are measured on a monthly basis and the quarterly results are published on GOV.UK with the Supplier's approval.</p> <p>1. Access to messaging platform / HTTP API uptime 24/7/365</p> <ul style="list-style-type: none"> • Target 99.95% <p>Rating:</p> <ul style="list-style-type: none"> • Good - 99.95% or above 24/7/365 • Requires improvement - 99.5% - 99.95% 24/7/365 • Inadequate - <99.5% 24/7/365

Data provided by the Notify team, or appropriately designated GDS staff member, and confirmed by the supplier.

2. Priority One* fault response time

- Initial response / acknowledgement time within 20 minutes
- Target restoration (work around) within 30 minutes from the time of initial response
- Target resolution within 1 working day from the incident reported
- Incident summary describing the root cause and future mitigations with agreed timelines, provided within 1 working day of resolution. The summary should be signed off by the Buyer.

Rating:

- Good - Initial response time 20 mins / Target restoration (work around) 30 mins / Target resolution 1 working day
- Requires improvement - Initial response time 20-60 mins / Restoration (work around) 4 hours / Resolution 1 working day
- Inadequate - Initial response time > 1 hour / Restoration (work around) > 4 hours / Resolution > 1 working day

Data provided by Notify team, or appropriate designated GDS staff member, and confirmed by the supplier.

* Priority One includes but is not limited to:

- HTTP API is completely unavailable or HTTP error rate above 0.5%
- Significant (affecting more than 5% of messages) issue or delay with provider being able to give messages to any or all UK MNOs
- Significant (affecting more than 5% of messages) issue or delay with provider being able to receive delivery receipts from any or all UK MNOs
- Significant (affecting more than 5% of messages) issue or delay with provider being able to pass MNO delivery receipts back to Notify
- Significant delays in users receiving text messages, for example 10% of messages being delivered slower than 10 minutes
- Other incidents where the Notify team decide there is significant impact to their users and communicate this should be treated as a Priority One incident.

3. Support response (outside of Priority Ones)

- Initial response time within 60 minutes within working hours
- Subsequent response times within 1 working day from initial response
- Target resolution within 5 working days
- If required from the Buyer, propose improvements with agreed

	<p>timelines provided, within 10 working days of resolution.</p> <p>Rating:</p> <ul style="list-style-type: none"> • Good - Initial response time within 60 minutes / Subsequent response times within 1 working day • Requires improvement - Initial response time 60-120 minutes and/or subsequent response time 1-2 working days • Inadequate - Initial response time > 120 minutes and/or subsequent response time >2 working days <p>Data to be provided by Notify team, or appropriate designated GDS staff member, and confirmed by the supplier.</p> <p>Assessment and penalties</p> <p>For each KPI that is rated lower than 'Good' the Supplier must provide a written report with explanation of the rating and the remedial action plans to bring performance back up to the target performance/ SLAs.</p> <p>This commentary will be published alongside the KPI result for that quarter. Progress on all remedial actions should be reported on an ongoing basis to the buyer, frequency determined by the Buyer.</p> <p>If the rating is 'Requires improvement' for 2 consecutive months, and/or the supplier does not complete more than 50% of all items on the latest remedial action plan, the Buyer reserves the right to withdraw payment until such improvements are made and confirmed by the Buyer.</p> <p>If the rating is 'Inadequate' for 2 consecutive months this constitutes a critical service failure. Any remedial action plans should be presented and agreed with the Buyer within 2 working days of identifying the critical service level failure. If these are not satisfactory or if the supplier has more than one critical service level failure for the duration of the contract, the Buyer can terminate the contract within the contractual notice period.</p>
Alternative clauses	<p>Not used</p>

Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>Within the scope of the Call-Off Contract, the Supplier will if applicable and pre-agreed with Cabinet Office comply with the Cabinet Office Travel & Subsistence Policy at Schedule 8.</p> <p>The Supplier shall conduct regular IT Health Check/penetration testing. The results and mitigation plans should be shared with the Buyer annually.</p>
Personal Data and Data Subjects	<p>Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1</p>
Intellectual Property	<p>Not used</p>
Social Value	<p>See Annex 3: Social Value, page 71</p>

1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a CallOff 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 (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13 .

Signed	FIRETEXT COMMUNICATIONS LTD	CABINET OFFICE
Name		
Title		
Signature		
Date		

- 2.2 The Buyer provided an Order Form for Services to the Supplier.

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 36 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, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.
- 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 set the Term at more than 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:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)

- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

- 2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- 2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'
- 2.2.3 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 Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.
- 2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.
- 2.5 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:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

- 4.1.2 apply all due skill, care and diligence in faithfully performing those duties
- 4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
- 4.1.5 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 as per clause 18.5 hereunder 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 14digit 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:
 - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their 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 portion of the 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:

9.2.1 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

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

9.2.3 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

9.2.4 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:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 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:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 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:

9.8.1 premiums, which it will pay promptly

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

10. Confidentiality

- 10.1 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 incorporated Framework Agreement clause

34. 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 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

- 11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

- 11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

- 11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

- 11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

- (a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
 - (b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
 - (c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract;
- and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer 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:

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 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:

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

11.7.2 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

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

11.8 Clause 11.6 will not apply if the IPR Claim is from:

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

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, 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:

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

12.1.2 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

12.1.3 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:

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

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

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 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

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

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

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

13.4 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 policies and all Buyer requirements in the Order Form.

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

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

- 13.6.1 the principles in the Security Policy Framework:
<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy:
<https://www.gov.uk/government/publications/government-securityclassifications>
- 13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:
<https://www.cpni.gov.uk/content/adopt-risk-managementapproach> and Protection of Sensitive Information and Assets:
<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
- 13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>
- 13.6.4 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:
<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>
- 13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:
<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
- 13.6.6 Buyer requirements in respect of AI ethical standards.
- 13.7 The Buyer will specify any security requirements for this project in the Order Form.
- 13.8 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.
- 13.9 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.
- 13.10 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 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 all reasonable endeavours, 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:

16.4.1 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

16.4.2 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 the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's 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:

<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:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 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 30 days' written notice to the Supplier, unless a shorter period is 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:

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

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover 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:

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

18.4.2 any fraud

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

if:

18.5.1 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

18.5.2 an Insolvency Event of the other Party happens

18.5.3 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:

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

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

19.4.3 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); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 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:

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

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

19.5.3 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

19.5.4 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

19.5.5 work with the Buyer on any ongoing work

19.5.6 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: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any 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 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 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 take the Term beyond 36 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:
 - 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer
 - 21.6.2 there will be no adverse impact on service continuity
 - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
 - 21.6.4 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:
 - 21.8.1 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
 - 21.8.2 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
 - 21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
 - 21.8.4 the testing and assurance strategy for exported Buyer Data
 - 21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 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:

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

22.1.2 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 30 consecutive days, 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 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

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:

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

25.5.4 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:

- | | |
|--------|---|
| 29.2.1 | the activities they perform |
| 29.2.2 | age |
| 29.2.3 | start date |
| 29.2.4 | place of work |
| 29.2.5 | notice period |
| 29.2.6 | redundancy payment entitlement |
| 29.2.7 | salary, benefits and pension entitlements |

- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29. 2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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.

29.3 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.

29.4 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.

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

29.5.1 its failure to comply with the provisions of this clause

29.5.2 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

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

29.7 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.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
 - 31.2.1 work proactively and in good faith with each of the Buyer's contractors
 - 31.2.2 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 CallOff Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

- 33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:

- **Service ID; 680677614553449**

- **Service Description; FireText Communications Limited**

FireText UK Secure (Official) SMS, RCS, WhatsApp and Advanced Messaging

Link to Service Description;

<https://redirect.contractawardservice.crowncommercial.gov.uk/g-cloud/services?id=680677614553449>

FireText Communications Limited

FireText UK Secure (Official) SMS, RCS, WhatsApp and Advanced Messaging

Omnichannel API Messaging: FireText provide a secure, trusted and easy-to-use messaging platform. UK-based cloud platform allowing 2-way SMS, RCS, WhatsApp and Advanced Messaging. Accredited to ISO27001, Cyber Essentials Plus and NHS DSP Toolkit standards. Platform is penetration tested by a CREST and NCSC CHECK accredited company on an annual basis.

Features

- Integrate with 4000+ other software platforms
- SMS
- RCS
- WhatsApp

- Omnichannel Messaging
- International Messaging
- Advanced Messaging
- Conversational Messaging
- Developer API
- Web platform

Benefits

- Reduce costs compared to other communication protocols
- Reduce missed appointments or meetings
- Improve speed of communication with end users
- Net Zero Carbon Neutral SMS
- Notify stakeholders and end users of time critical information
- Align with Digital by Default ethos
- UK located private cloud servers
- Easily Integrated Messaging
- Use via existing software platforms
- Hand-Holding Support provided in the UK

Service documents

[Pricing document](#)

PDF

[Service definition document](#)

PDF

[Terms and conditions](#)

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform 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:

- [Pricing document](#)

PDF

- The total value of this Call-Off Contract is **Up to £38,681,500 (exc. VAT)**
- The total value Includes an optional 12 month extension (pricing to be reviewed 02/01/2024)
- There is no provision to review SMS/fragment UK pricing during the initial 12 month term of contract.
- The supplier's prices are **fixed** for 12 months.

Schedule 3: NOT USED

Schedule 4: NOT USED

Schedule 5: NOT USED

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) 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 Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none">• 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 <p>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.</p>

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, substantially in the form set out at Schedule 3, 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	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> • 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.
Controller	Takes the meaning given in the UK GDPR.
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 Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE')
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 the 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: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • 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 <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • 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 <p>Majeure at the time this Call-Off Contract was entered into</p> <ul style="list-style-type: none"> • 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	<p>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).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.13 together with the Framework Schedules.</p>
Fraud	<p>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</p>

	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 Clause 2 (Services) 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.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
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.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
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.

Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
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	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less
-------------------------	--

Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • 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	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
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 Buyer's possession before the Start date.

Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
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 Schedule 6.
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	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.

Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	<p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ 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.

Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's highperformance 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).

Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
---------------------------------	---

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 GCloud 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 Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
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-controlscheck-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 GCloud 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.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
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.

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

Annex 1: Processing Personal Data

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

- 1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED]
- 1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex;

Descriptions	Details
Identity of Controller for each Category of Personal Data	The Buyer is Controller and the Supplier is

	<p>Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>SMS Providers for GOV.UK Notify, a multi-channel digital communications platform that UK public sector service teams can use to send emails, text messages, and letters to users of their service. These messages will typically be status updates, requests for action, receipts of applications or supporting information, and reminders.</p>
Duration of the Processing	<p>Processing is typically complete within 7 days, however there is a potential for service teams to request Notify to retain their notification data for up to 90 days so they can subsequently respond to their users queries about messages they were sent in the past.</p> <p>Third party suppliers to Notify, that distribute the notifications will retain the data for up to 12 months for audit and billing purposes.</p>
Nature and purposes of the Processing	<p>Notify collects personal data only for the purposes of processing notifications and reporting on the success or failure of delivery</p> <p>Notify uses a number of third party suppliers to distribute the notifications to recipients.</p> <p>Once the relevant retention period has been reached, data is deleted from Notify and from the third party suppliers.</p> <p>While Notify holds data, service teams that have provided the data in their role of data controller, can see the data within Notify and access the delivery outcomes.</p> <p>The purposes for sending notifications to public sector service users are many and varied, but generally fall into the categories of progress updates about transactions, reminders of appointments or renewals, alerts about guidance changes or events.</p>
Type of Personal Data	<p>All notifications will contain either an email address, a mobile phone number, or a physical address.</p> <p>Additionally there can be personalisation in the notifications, which can include people's names, reference numbers, dates of events / appointments etc.</p>

Categories of Data Subject	Includes but is not limited to: staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students pupils, members of the public, users of a public sector websites.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Personal data must be automatically deleted at the end of the data retention period, which for Notify and it's third party providers ranges between 3 days and 12 months.

Annex 2: Joint Controller Agreement - Not used

SCHEDULE 8

Cabinet Office T&S Policy

All expenses must be agreed in advance with the Cabinet Office, and all claims should be in line with the Cabinet Office expenses policy. All claims should be supported by receipts, and as a general rule the lowest cost travel option should be chosen.

Supplier organisations must also comply with the following:

1) Travel rates

Cabinet Office will reimburse any essential and necessary travel related expenses that you incur through carrying out work on behalf of the Department. We will pay for all excess costs you incur travelling on official business. Official travel is defined as a journey that you:

- have to make in the performance of your duties
- make to or from a place you have to attend in the performance of your duties.

This will include travel between offices if you have more than one base. It excludes daily commuting to and from your normal place of work under this contract.

The lowest cost of travel should be chosen for your journey. Specific rules apply to chosen mode of travel.

Rail Travel

All rail travel must either be booked at standard or economy class, or at the lowest fare (even if this is 1st Class). Anytime or open tickets should only be booked when this is either the lowest fare, or there is a clear business justification.

Air Travel

All air travel must be booked at standard or economy class, and on lowest fare. If the flight has a flying time of over 5 hours, Premium Economy or Business Class (if Premium Economy is not available) on lowest fare, is acceptable.

Taxis

You may use a taxi for official business travel only when:

- you are outside of normal working hours (before 6am and after 9pm)
- no other suitable method of public transport is available, and
- travel by private vehicle or self-drive hire car is not possible and/or is not cost effective, and either:
 - you are transporting heavy luggage or official business equipment, or
 - the saving of official time is important and can be justified on cost grounds.

All taxi fares should be receipted.

Hire a self-drive car

We will refund the costs of a self-drive car, if:

- this is cheaper and /or more appropriate than using public transport, and
- you have a current driving licence.

You should hire the least expensive and smallest car necessary for your official journey, and be able to demonstrate value has been achieved through the hire

decision.

If you use the hire car for any private travel or if you transport any non-official passengers you must pay for your own petrol and make sure that you have your own private fully comprehensive insurance cover

Personal Mileage Allowance

Claims submitted for travel should be based on actual costs incurred and capped at the rates for civil servants.

The standard rate payable for most official business travel is the - Public transport rate – Car 26p per mile, Motor cycle or motor bike 24p per mile, Bicycle 20p per mile.

Where travel by public transport is impossible or more expensive than using your own car, the cost of hiring a car was more expensive than using your own vehicle or you have to drive the car you own due to a disability the first 10,000 miles in a tax year are paid at 40p, over this the rate is 25p.

2) Subsistence rates

UK Lodging rate for rented accommodation

Ceiling - £37 per night.

UK Hotel accommodation rate

Ceiling for bed and breakfast:

UK

£150 - London (from centre out to the M25 motorway ring road)

£110 - Major cities (Aberdeen, Birmingham, Belfast, Bristol, Cardiff, Coventry, Edinburgh, Glasgow, Harlow, Leeds, Liverpool, Manchester, Middlesbrough, Newcastle, Oxford, Portsmouth, Reading, Sheffield, York)

£100 - Elsewhere

International

£170 - Tier 1, New York, Washington DC, Muscat-Ruwi, Oslo, Geneva, Ottawa, Strasbourg, Tbilisi, Stockholm, Paris, Belgium, Brussels, Amman

£130 - Tier 2, Elsewhere.

If the cost of breakfast is not included in the accommodation charge a separate payment may be made. The room and breakfast costs overall should remain within the above ceiling. If breakfast cannot be taken because of an early start, a separate breakfast allowance may be paid.

UK Meal allowance

If working more than 5 miles away from your normal place of work you are entitled to claim for:

one meal if away for over 5 hours

two meals if away for 10 to 12 hours

three meals if away for over 12 hours

The ceilings within which you may claim are:

£5 - breakfast

£5 - lunch

£18 - dinner

£23 - combined lunch and dinner

These costs cover food and drink and must be supported by receipts.

Modest expenditure on alcoholic/soft drinks is permissible but if a meal is provided by a third party then a claim solely for alcoholic/soft drinks must not exceed £4 and should be supported by receipts.

UK Personal Incidental Hotel Expenses - £5 per night

This payment is flat rate. It may be claimed to cover out-of-pocket personal expenses (for example laundry, tips, phone calls home) incurred during overnight stays in an hotel or residential training course accommodation. The payment may not be made in conjunction with the flat rate payment for staying with friends or relatives.

UK Staying with friends or relatives rate - £25 per day

This is a flat-rate payment and takes account of all aspects of a 24 hour stay: for example, accommodation, meals, phone calls home and transport between temporary office and place of temporary residence. It may not be claimed in conjunction with the payment for Personal Incidental Expenses.

Overseas rates

Overseas subsistence for hotels, meals and local home to office travel

A separate rate is set for each [country](#) to cover meals, accommodation and hotel to office travel. Travel from the airport to hotel will be reimbursed separately. Please discuss with Cabinet Office before travelling to agree rates.

Overseas staying with relatives or friends rate

If you stay with friends or relatives overseas you will receive the residual element of the subsistence allowance payable for the [country](#). It may not be claimed in conjunction with Overseas Personal Incidental Expenses.

Overseas personal incidental hotel expenses

days 1 to 4 = £5 per day

day 5 onwards = £10 per day

This is a flat rate. It may not be claimed in conjunction with the payment for staying with relatives or friends overseas.

ANNEX 3: SOCIAL VALUE

RFC: SOCIAL VALUE REQUIREMENT (The Contracting Authority (Buyer))

8. Social Value (Social Value Act)	<p>Theme: Fighting Climate Change</p> <p>Policy Outcome: Effective stewardship of the environment</p> <p>Award Criteria: You will be assessed against your ability to;</p> <ol style="list-style-type: none">Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions.Influence staff, suppliers, customers and communities through the delivery of the contract to support environmental protection and improvement. <p>Using a maximum of 500 words, describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria.</p> <p>Please include:</p> <ul style="list-style-type: none">your 'Method Statement', stating how you will achieve this and how your commitment meets the Award Criteria, and;a timed project plan and process, including how you will implement your commitment and by when. Also, how you will monitor, measure and report on your commitments/the impact of your proposals. <p>You should include but not be limited to:</p> <ul style="list-style-type: none">timed action planuse of metricstools/processes used to gather datareportingfeedback and improvement transparency
---	---

SOCIAL VALUE: REPORTING

Mandatory Requirement;

FIRETEXT COMMUNICATIONS LTD will provide a quarterly report in writing on progress towards their targets, as described in the RFC response, above ****REDACTED****.

Frequency;

Quarterly over duration of the contact - (dates due);

1 April

1 July

1 October

2 January

31 March

Acceptance criteria (to be reviewed and formally accepted in writing by delegated person(s) within GDS/CO);

0 - Not met

1 - Partially Met

2 - Met

3 - Exceeded expectations

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]