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

Order Form Template

CALL-OFF REFERENCE:	AGEMCSU/TRANS/23/1689
THE BUYER:	NHS Black Country Integrated Care Board Integrated Care Board
BUYER ADDRESS	NHS Black country Integrated Care Board Civic Centre St Peters Square Wolverhampton WV1 1SH
THE SUPPLIER:	BT PLC
SUPPLIER REFERENCE	BTNS370088
SUPPLIER ADDRESS:	1 Braham Street, LONDON, E1 8EE
REGISTRATION NUMBER:	01800000
DUNS NUMBER:	22 701 5716
SID4GOV ID:	N/A

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 12/04/2024. It's issued under the Framework Contract with the reference number RM6116 for the provision of Network Services.

CALL-OFF LOT(S):

- Lot 3b: Communication Platform as a Service

[redacted]

CALL-OFF INCORPORATED TERMS

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

1. This Order Form, including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6116
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6116
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)

    - Call-Off Schedules for RM6116
        - Call-Off Schedule 5 (Pricing Details)
4. CCS Core Terms (version 3.0.11)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6116
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

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

CALL-OFF START DATE: 1st April 2024

CALL-OFF EXPIRY DATE: 31st March 2025

CALL-OFF INITIAL PERIOD: 12 Months

CALL-OFF OPTIONAL EXTENSION PERIOD N/A

[redacted]

CALL-OFF DELIVERABLES
Option A:

Requirement:

Please see below NHS Black Country ICB monthly average usage for SMS:

ICS/ICB	Renewal Date	Average Monthly Volume 22/23
NHS Black Country Integrated Care Board	30/03/2024	580480

Suppliers must also confirm the following Pass | Fail questions (any supplier receiving a Fail will be excluded from this procurement process)

Question number	Question	Pass	Fail
Q.01	Please confirm you are able to integrate into Clinical Systems i.e., EMIS, TPP, Accurx, Netcall etc.?		
Q.02	Please confirm you can report/give a breakdown on Cost Centres by API?		
Q.03	Please confirm you can supply a SMTP Email to SMS API?		
Q.04	Please confirm you are using direct UK message Routing?		
Q.05	Please confirm you have a process for migration from existing supplier to you		

Q.06 We require Supplier to Confirm price per message and also any additional costs. i.e. cost of API's etc.	Included in excel below

1 year - Renewal date: 1st April 2024 to 31st March 2025

[redacted]

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is Approximately £166,860.00 (approx. based on last year's SMS average).

VALIDATION REFERENCE: 175

[redacted]

CALL-OFF CHARGES
Option A: the Charges for the Deliverables

[redacted]

Suppliers must also confirm the following Pass | Fail questions (any supplier receiving a Fail will be excluded from this procurement process)

Question number	Question	Pass	Fail
Q.01	Please confirm you are able to integrate into Clinical Systems i.e., EMIS, TPP, Accurx, Netcall etc.?		
Q.02	Please confirm you can report/give a breakdown on Cost Centres by API?		
Q.03	Please confirm you can supply a SMTP Email to SMS API?		
Q.04	Please confirm you are using direct UK message Routing?		
Q.05	Please confirm you have a process for migration from existing supplier to you		

Q.06 We require Supplier to Confirm price per message and also any additional costs. i.e. cost of API's etc.	

1 year - Renewal date: 1st April 2024 to 31st March 2025

[redacted]

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES
None

PAYMENT METHOD
Invoices will be raised by the provider and invoices paid in arrears, no later than 30 days from the date of invoice.

Payment made by BACS.

BUYER'S INVOICE ADDRESS:

NHS Black country Integrated Care Board
QUA PAYABLES M875
PO BOX 312
Leeds
LS11 1HP

Invoices: sbs.apinvoicing@nhs.net

BUYER'S AUTHORISED REPRESENTATIVE

[redacted]

BUYER'S ENVIRONMENTAL POLICY

https://blackcountry.icb.nhs.uk/

BUYER'S SECURITY POLICY

https://blackcountry.icb.nhs.uk/

[redacted]

[redacted]

Address: 3 Snowhill, Snowhill Queensway, BIRMINGHAM, B4 6GA

SUPPLIER'S CONTRACT MANAGER

[redacted]

PROGRESS REPORT FREQUENCY
N/A

PROGRESS MEETING FREQUENCY
N/A

KEY STAFF
N/A

KEY SUBCONTRACTOR(S)
N/A

COMMERCIALLY SENSITIVE INFORMATION
BT is providing information in commercial confidence and considers that the information would be exempt from disclosure under the FOIA. BT expects the Customer Authority to respect that confidence. Section 41 of the FOIA exempts the Customer Authority from disclosing that information as the disclosure (otherwise than under the FOIA) would constitute an actionable breach of confidence.

Disclosure of the information would also be commercially prejudicial to BT's interests and accordingly exempt from disclosure by virtue of section 43 of the FOIA.

The following terms apply from date of issue:

- All BT pricing – 7 years
- All BT service description/service offer information – 7 years
- BT security process information – 7 years
- BT disaster recovery information – 7 years
- All personal data (under GDPR) – Perpetual

SERVICE CREDITS
N/A

ADDITIONAL INSURANCES
N/A

GUARANTEE
N/A

[redacted]

SOCIAL VALUE COMMITMENT
Not applicable

For and on behalf of the Supplier:	For and on behalf of the Buyer:
[redacted]	[redacted]

[redacted]

BT Security Management Plan

Supporting all CCS framework and DPS agreements

Issue 4.0 (17/11/2023)

[redacted]

Frameworks

Security Management Plan

OFFICIAL Handling Rules	
Sensitivity	APPROPRIATLEY CLEARED STAFF WITH A NEED TO KNOW ONLY
Physical Storage	Protect in line with local guidance on open-plan working and clear desk principles. This may include: protecting physically within a secure building by a single lock (e.g. a locked filing cabinet, locked drawer or container); not leaving papers on desks or on top of cabinets overnight.
Electronic Storage	General security controls.
Printing	printing facility: collect immediately – Secure Printing Facility preferable
E-mail	Can be sent as an encrypted document WinZip/7Zip with 256 bit AES encryption as a minimum. CJSM or Secure internal system.
Copying	Permitted – but make only as many copies as you need, and control their circulation
Disposal	Information marked OFFICIAL must be disposed of with care, either using a secure disposal bin or by shredding using an approved crosscut shredder.
Distribution	A Need to Know basis

[redacted]

Contents

[redacted]

1. Document Controls

1.1. Confidentiality Statement

1.2. Document Control

Author: BT Security

BT Frameworks Contract Manager

[redacted]

Document history

Issue	Date	Notes
1.0	9 Aug 19	Released version
2.0	22 Nov 19	Monor text changes
2.1	October 20	Review and incorporation of new BT logo
3.0	8 Feb 2022	Review and changes
4.0	17 Nov 2023	Review and updated to cover all frameworks

[redacted]

1.3. References

	Document Title	Date and Version
[1]	CCS Framework and DPS Agreement Call-Off Schedule 9 (Security) Part A	version 1.0
[2]	ISO/IEC 27001 (Information Security Requirements Specification)	Nov 2013
[3]	ISO/IEC27002 (Information Security Code of Practice)	Nov 2013
[4]		

2. Introduction

2.1. Purpose

The purpose of this document is to maintain the security of the contract in line with the contracted security obligations

2.2. Security Plan Scope

This Security Management Plan (SMP) defines the security measures that are implemented, and maintained, by BT. BT will maintain the adherence to the contracted security measures. This SMP will at all times during the life of this Call-Off Contract comply with the Buyer requirements as defined in the **Call-Off Schedule 9 (Security) Part A**

[redacted]

3. Supplier Approach to Security

3.1. BT's Approach to Security

The BT Corporate Security ISMS (Information Security Management System) has been certified to ISO 27001:2013 [2] for 'Critical information to enable the management of the security services [listed below], that protect BT provides to BT and specific customer contracts' LRQA certificate LRQ0962885. The scope of the certificate includes:

- BT Corporate Security Standards and Policies.

N.B. In accordance with ISO27001, BT inserts clauses into third party supplier contracts that the third party implements the same personnel security procedures as BT. Compliance is audited by separate specialists not involved in the operational running of the system. Where appropriate BT will create a 'flow-down' SAL, based upon the one it has received, to ensure customer's security requirements and specifications are accurately reflected in its contracts with suppliers

[redacted]

4. Information Security Policy

4.1. Information Security Policy Statement

4.1.1. Management Approval

All security policies are approved at an appropriate level within BT. While overall management commitment is provided by the CEO, specific areas such as Personal Security in BT's Acceptable Use policy and HMG Security in BT's Guidance for UK Government Security are approved by specialists representing those areas.

4.2. Review of Information Security Policy

Both BT Internal Security Policies and Customer Specific policies are stored in a centralised, electronic storage system. This ensures all parties are using the same most up to date policies. All policies have a designated owner, are reviewed/revalidated on a regular basis and maintain a change control history.

5. External Parties

5.1. Identification of Risk Related to External Parties

BT runs a Supply Chain Security (formerly known as Procurement & Security Gate) process. This evaluates the relationship BT has with each of its third parties to ensure that appropriate risks are identified and controls put in place. This process includes ensuring appropriate clauses are included within third party contracts as well as auditing third parties to ensure appropriate controls are in place. Where Customer specific obligations require flowing down to third parties, BT is working with the contract commercial team to achieve this.

5.2. Addressing Security when Dealing with Customers

In a Business to Business environment, this covers the security around electronic bonding of systems such as ticketing and e-mail. BT's Third Parties policy deals with access to BT Assets by a BT Customer. This includes the technical controls such as user accounts and passwords as well as procedural controls to ensure Customers handle any BT information appropriately.

5.3. Addressing Security when Dealing with Third Party Agreements

In accordance with ISO27001, BT inserts clauses into third party supplier contracts stating that the third party implements the same personnel security procedures as BT. Compliance is audited by separate BT Group specialists.

5.4. Special Security Requirements for External Parties

Where a third party may require a special requirement in order to deliver its service, a risk assessment will take place using the BT Group Supply Chain Security (formerly known as Procurement & Security Gate) process to consider the risks and any appropriate controls to require to mitigate the risk.

[redacted]

6. Human Resources Security

6.1. Prior to Employment

6.1.1. Roles and Responsibilities

All individuals working on the contract have clear roles and responsibilities issued in line with BT HR guidelines and policies. Individual's roles within the contract have been documented as necessary within the Contract Handbook or equivalent.

6.1.2. Screening

All UK BT staff and contractors are cleared to an equivalent of the HMG BPSS through pre-employment checks. This involves:

* Verification of Identity;

* Verification of nationality and Immigration Status;

* Verification of Employment History;

* Verification of Criminal Record (unspent convictions only).

6.1.3. Terms and Conditions of Employment

All individuals working on the Buyer Contract have been recruited and managed via BT's HR guidelines and processes. This includes pre-employment checks, mandatory security training. Employees and contract staff are subject to a formal disciplinary process.

6.2. During Employment

6.2.1. Management Responsibilities

BT's Acceptable Use policy: Line Manager Responsibilities ensures that oversight of individual's security is appropriately provided. This includes ensuring mandatory security training is completed, physical asset security guidelines are followed and individuals understand their responsibilities involving fraud prevention.

BT's Guidance for UK Government Security provides management oversight of individuals who hold vetting and clearance to ensure this is maintained as necessary.

6.2.2. Information Security Awareness, Education and Training

All BT staff must successfully complete mandatory training as part of their induction including "year on year" compliance. Security training is mandatory for all employees and is conducted online.

6.2.3. Security Training

All BT staff must undergo mandatory training as part of their induction and "year on year" compliance. This training includes modules on all aspects pertinent to the role of the individual

[redacted]

and where they work within BT. Security training is mandatory for all employees and is conducted online. BT's standard security-awareness training will be augmented with customer-specific material including but not limited to such details as:

- handling and disposal requirements,
- when PSTN can / cannot be used,
- when standard BT email can / cannot be used and when something like CJSM (mail) is appropriate,
- working on customer sites.

6.2.4. Disciplinary Process

The BT disciplinary process applies a robust but fair process of investigation which is clearly documented and available to all employees. All staff are made aware of this process and their responsibilities when recruited.

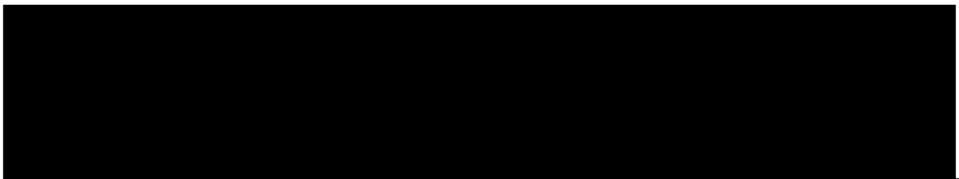
6.3. Termination or Change of Employment

6.3.1. Termination Responsibility

For individuals who leave BT Group, it is the line manager's responsibility to ensure that BT HR guidelines and policies are followed. BT's Acceptable Use policy: People Manager Requirements provides a link to the Leavers Checklist, which must be followed.

6.3.2. Return of Assets

BT's Acceptable Use policy: People Manager Requirements provides a link to the Leavers Checklist which must be followed by line managers when an employee leaves BT. This includes logging the return of all assets as maintained on BT Groups eOrganisations asset database.



7. Physical and Environmental Security

7.1. Secure Areas

7.1.1. Physical Security Perimeter

BT Buildings as well as physical and environmental security areas are regularly assessed and access control is applied throughout the company. BT employ rigorous security standards at all of its buildings. This protection is implemented using:

* CCTV;

* alarms;

* security reception staff;

* all staff have proximity cards that can be programmed to entry;

7.1.2. Physical Entry Controls

BT manages a centralised access control system (BASOL) across its entire building estate. Building are zoned to enable access to individual zones to be allocated on the individuals based on their need for access. Zones are owned by local representatives. Permanent and contract staff are issued proximity cards to allow access. Zones may be accessed by card only or a combination of card and PIN.

Access to zones and a permanent and temporary basis is managed through a web based order system. Zone owners are responsible for assessing, authorising and auditing user access.

BT's Physical Security policy describes the policy for protecting BT's people, assets and environment including network infrastructure, systems and processes from the following threats: theft, burglary, arson, tampering, sabotage or terrorism.

7.1.3. Securing Offices, Rooms, and Facilities

Section 7.1.2 above describes how offices, rooms and facilities are zoned to allow granular access control based on an individuals need for access.

7.1.4. Protecting Against External and Environmental Threats

All buildings are audited on a regular basis by BT Physical Assurance managers. Buildings are categorised based on their use. Appropriate physical and environment defences are applied to the building itself or areas of the building to protect the assets within. BT has dedicated Physical Assurance Managers to assess and manage areas requiring higher levels of protection including those to protect HMG assets as described in BT's Guidance for UK Government Security.

7.1.5. Working in Security Areas

BT's Acceptable Use policy describes baseline personal security for working in all BT offices. This includes display of ID badges, clear desk policy and locking of computer screen when away from

[redacted]

the desk. BT's Guidance for UK Government Security describes additional controls including locking protectively marked material away when not at your desk and awareness of how to report and escalate any security issues. Additional Information has been added to local Office Security Instructions (OSI's) to fulfil the requirements of the contract.

7.1.6. Public Access, Delivery and Loading Areas

Public access will not be permitted to any BT areas used to manage the Framework Contract.

Assets used to deliver the Framework Contract will be transported based on procedures developed to meet the specific requirements of the Contract. Assets should not be left unattended in unprotected delivery and loading areas.

[redacted]

8. Asset Management

8.1. Responsibility for Assets

8.1.1. Inventory of Assets

Following the controls within ISO27001 BT will ensure an inventory of assets pertinent to the contract is drawn up and maintained. Changes to these assets will be strictly controlled under change management with security input.

BT maintains a single logical inventory of assets used within the Buyer solution. This is used to underpin a full range of ITIL service management processes. Procedures for handling assets have been developed and implemented in accordance with any customer specific requirements as per the contract.

An inventory of Personal assets including laptop computers and mobile phones are maintained at a BT Group level. This inventory supports a number of Human Resource (HR) processes including the company leavers process.

8.1.2. Ownership of Assets

Assets used within the Customer Solution are owned by BT. The day to day responsibility for handling and maintenance of these assets is described in contracts operational process and procedures.

Personal assets including laptop computer and mobile phone are owned by the individual. The logical configuration and protection including preventative security measures are maintained through companywide policies and procedures. Management of personal assets is covered by BT's Acceptable Use policy.

8.1.3. Acceptable Use of Assets

BT's Acceptable Use policy describes the acceptable use of the internet, e-mail and messaging systems. BT's Acceptable Use policy and BT's Guidance for UK Government Security specifically describes the handling of HMG assets. In addition to this, procedures for handling assets have been written and implemented in accordance with any customer specific requirements as per the contract.

8.2. Information Classification

8.2.1. Classification Guidelines

BT has four levels of classification for its internal information. These include Public, General, Confidential and Highly Confidential. These are described in BT's Acceptable Use policy. BT classifies HMG assets using the UK Government Security Classification Policy (GSCP). This is described in BT's Acceptable Use policy and BT's Guidance for UK Government Security.

8.2.2. Information Labelling and Handling

BT will handle and label information as described in BT's Acceptable Use policy and BT's Guidance for UK Government Security.

BT uses best practice on how to handle information in line with the GSCP and in accordance with any customer specific requirements as per the contract.

9. Operation of the Plan

9.1. Operational Security

9.1.1. General

This section defines the general areas of consideration when seeking compliance or alignment with ISO27001.

- Scope. Will be defined in the related ISMS or Security Policy for any solutions/services or offerings already certified.
- Security organisation

The following sections define specific areas within the ISO27001 standard, which are given due consideration.

9.1.2. Asset Management

Following the controls within ISO27001 BT will ensure an inventory of assets pertinent to the contract is drawn up and maintained. Changes to these assets will be strictly controlled under change management with security input to include aspects such as specific disposal requirements/procedures that must be met.

- All employees, contractors and external party users return all contract specific organisational assets in their possession upon them moving off the contract.
- Procedures for handling assets will be developed and implemented in accordance with contract; e.g.:
  - how information is to be transferred using removable media,
  - criteria for when secure email (e.g. CJSM) must be used,
  - use of cross-cut shredders; i.e. SEAP 8100 approved shredder with a shred of 4mm x 15mm or less.
- Media will be disposed of securely when no longer required, using change control.
- BT operates a secure asset disposal process compliant with HMG IA Standard 5 [5].

NB: **Also found in ISO27001 SOA section A.8.x**

9.1.3. How Customer Data is Kept Secure and Separated from other Customer's Data

BT has implemented a data regime as shown below.

Access to Customer operational data is stored in the Primary and backup datacentres but will be viewed from the operations team. Operational data is encrypted end-to-end between the managed routers. The types of data BT holds is:

- Structured Information – Events/logs from the managed customer devices.
  - Events/Logs are held on management platforms that are housed in approved facilities
  - information relating to tickets Is held within BT's assured management system, either in the dedicated Ticketing system or the Configuration management system

[redacted]

- Ticketing systems are designed for a multi-tenanted environment where RBAC is used to define who has access to what based on a need-to-know / need-to-see basis.
- A user must hold a suitable clearance as an absolute pre-requisite for access to the platform; additionally, for access to customers' information an agreed clearance Level is required.
- Procedures exist to ensure the appropriate clearance is held.
- Access is regularly revalidated.

- Unstructured Information – the contract, who to send invoices to, design material
  - Is typically held in SharePoint
  - Sensitive material is encrypted using AES256-bit encryption
  - Complex Passphrases are used to encrypt material
  - Roll-Based Access Control (RBAC) is also used for access to individual customer's data
- Where data has to be extracted for Openreach the exact details will be agreed with the customer and will be obfuscated where appropriate and possible.

NB: **Also found in ISO27001 SOA section A.9.x**

9.1.4. Cryptography

BT's PSN Encryption Overlay Services (EOS) and PSN PKI may be use to encrypt traffic across the management links.

NB: **Also found in ISO27001 SOA section A.10.1**

9.1.5. Information Security Policies

The Information Assurance Manager (IAM) if assigned will liaise with the customer to determine any specific information security policies that are over-and-above BT's mandatory policies. These will be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness by both BT and the customer.

NB: **Also found in ISO27001 SOA section A.5.x**

9.1.6. Organisation of Information

The commitment of senior management to information security is provided from the CEO of BT by a Security Directive from the CEO of BT
https://intra.bt.com/bt/security/securitypolicy/policy/Pages/index.aspx

The ethos of this security directive is embedded into all policies and processes operated by BT.

NB: **Also found in ISO27001 SOA section A.6.x**

9.1.7. Access Control

BT will audit the Joiners, Movers and Leavers process which is documented within the Service Handbook.

9.1.8. Physical and Environmental

BT Buildings as well as physical and environmental security areas are regularly assessed and access control is applied throughout the company.

[redacted]

BT employs rigorous security standards at all of its buildings. This protection is implemented using:

- CCTV;
- alarms;
- security reception staff at certain sites;
- all staff have proximity cards that can be programmed to entry;
- awareness training for all staff.

NB: **Also found in ISO27001 SOA section A.11.x**

9.1.9. Operations Security

Operating procedures affecting security are audited and the results made available to all users who are working on the contract. Staff working on the contract will be required to confirm they have read the relevant procedures as part of the joiners/leavers process.

NB: **Also found in ISO27001 SOA section A.12.x**

9.1.10. Security Monitoring

- Security Monitoring of the Management Platform is undertaken depending upon contractual obligations.

NB: **Also found in ISO27001 SOA section A.12.4.x**

9.1.11. Supplier Relationships

BT audit the sub-contractors/3rd party management to ensure the contractors are compliant with ISO27001 in line with the Contract and good industry practice.

NB: **Also found in ISO27001 SOA section A.15.x**

9.1.12. Information Security Incident Management

Security Incident processes and procedures are documented within the service handbook. A log of security incidents is kept for the customer contract.

NB: **Also found in ISO27001 SOA section A.16.x**

9.1.13. Security Aspects of Business Continuity Management

A Framework BC/DR plan will apply for the Buyer Contract where a bespoke BC/DR has not been requested by the Buyer . This will be reviewed annually.

9.1.14. Systems Acquisition, Development and Maintenance

BT employ procedures and processes in line with ISO27001 to ensure we have rules for development and changes and these are controlled via formal change control. Where changes are made we will ensure procedures are in place to ensure proper reviews and testing.

NB: **Also found in ISO27001 SOA section A.14.x**

9.2. Accreditation

Accreditation if required is undertaken by the Buyer.

[redacted]

9.3. Amendment and revision

BT will review, test and update the ISMS (if required) and the Security Plan at least annually to reflect:

- emerging changes in Good Industry Practice;
- any change or proposed change to the Contractor System, the Services and/or associated processes;
- any new, perceived or changed Breach of Security; and
- any reasonable requests by the Customer Authority.

BT will provide the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS (if required) and Security Plan in light of any findings. The results of the review shall include:

- suggested improvements to the effectiveness of the ISMS;
- updates to the risk assessments;
- proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and
- suggested improvements in measuring the effectiveness of controls.

10. Security Lifecycle

10.1. Maintaining the Security Plan

BT will review and update the Security Plan annually to reflect any:

- change or proposed change to the Framework and the products offered and associated processes;
- new, perceived or changed Breach of Security; and
- contractual change requests.

Contractual change requests will be managed by agreed mechanisms between BT and the Buyer. The plan will be reviewed outside the annual plan should there be any incident that requires an immediate change to process.

11. Annex A: Glossary of Terms

Acronym	Description
BPSS	Baseline Personnel Security Standard
HMG	Her Majesty's Government
IAM	Information Assurance Manager
IL	Impact Level
ITHC	IT Health Check
RA	Risk Assessment
NMC	Network management Centre
RTP	Risk Treatment Plan
SC	Security Check
SIRA	Security & Information Risk Advisor
SLA	Service Level Agreement
SoA	Statement of Applicability
SyOPs	Security Operating Procedures

END OF DOCUMENT

OFFICIAL

[redacted]

Smart Messaging (Tailored Service)

This Service Offer comprises of Services specific to Lot 3b. Lot 3b covers the provision of a range of Network Services (including hardware) commodity defined deliverables through a standardised and simplified catalogue.

This Service Offer is for Smart Messaging Tailored Service as defined in RM6116 Framework Schedule 1 (Specification), Paragraph 2.7.

Table of Contents

[redacted]

Smart Messaging (Tailored Service)

Service Offer Reference Number: RM6116-BT-Lot3b-039

Lot: 3b

Smart Messaging (Tailored Service) Effective Date: 1 March 2024

Smart Messaging (Tailored Service) Expiry Date:

Smart Messaging (Tailored Service) Service Description

The Smart Messaging platform, complete with its suite of applications and APIs, is designed to help organisations fulfil their messaging requirements across multiple channels, such as SMS, voice, email and Rich Communications Services, "RCS".

It is a web-based tool that simultaneously supports the composition and management of outbound and inbound campaigns. Organisations will be able to build contact databases, personalise messages, schedule campaigns and manage opt-in and opt-out lists to ensure regulatory compliance.

The platform also provides a comprehensive set of APIs to enable development, migration and automation of existing and new services, enabled across multiple channels.

The content of this Service Offer will be incorporated into the Call-Off Order Form on completion of an Order for the described services.

Smart Messaging (Tailored Service) Service Summary

The Supplier will provide the Buyer with a right to access and use its communication platform and messaging service, delivered via the Buyer Portal, as set out in any applicable Order Form up to the point of the Service Management Boundary as set out in Paragraph 1. The Service comprises:

(a) the Standard Service Components; and

(b) any of the Ancillary Services,

Smart Messaging (Tailored Service) Standard Service Components

The following Standard Service Components are available in accordance with the details set out in any applicable Order Form:

(a) **Buyer Portal**: access to the Buyer Portal via any compatible web browser that has internet access, to enable each Administrator to:

(i) access and use the Ancillary Services the Buyer has selected via the Buyer Portal;

(ii) register and de-register Users and their permissions;

(iii) manage the configuration of Users' profiles, including the groups or teams to which they belong and their access permissions to the Buyer Portal;

(iv) set up and manage contacts, groups and lists;

[redacted]

(v) set up and manage configuration and consent settings; and

(vi) access historical and real-time reporting on the usage by Users of the Service.

(b) **Introductory training**: an introductory webinar training session for the Buyer's Administrator(s) on how to use the Buyer Portal.

(c) **Guidance Documentation**: set up guides, user and maintenance guides, manuals and other documentation in relation to the use or operation of the Service via the Buyer Portal.

(d) **Technical Support**: technical support by telephone or email to the Service Desk during Working Hours to assist with account provisioning, basic troubleshooting, general platform queries, password resets, diagnostics, software workarounds and other non-critical requests.

(e) **Emergency Hotline Support**: access to an emergency telephone hotline, available 24 x 7 x 365, to report and seek support on Critical Incidents or Major Incidents and unplanned outages.

Smart Messaging (Tailored Service) Ancillary Services

The following Ancillary Services are available; these are optional services that enhance or otherwise supplement or support the delivery and/or the functionality of the Service:

(a) **Messaging Features**:

(i) **WebSMS**: standard web-based UK and international SMS messaging service for an unlimited number of Users (the "WebSMS Module"), which includes:

- message personalisation;
- scheduled delivery of messages; and
- simple usage reporting.

(ii) **WebSMS+**: includes all the features of the WebSMS Module, as well as additional functionality such as:

- ability to send bulk SMS to contacts, groups or lists;
- setting Message validity period and delivery times;
- Message personalisation and templates;
- Message cloning;
- setting frequency for recurring campaigns;
- permission management to enable End Recipients to opt-out from Messages; and
- blacklisting and whitelisting.

(iii) **Inbound**: this module allows the Buyer to receive an incoming Message sent from a mobile device (the "**Inbound Module**"). It can automatically sort, and respond to the Message, based on the Message's content.

(iv) **Inbound+**: this module includes all of the features of the Inbound Module, but adds real-time tracking, detailed reports, permission-management, and easy integration into the Buyer's existing systems, such as customer relationship management (CRM) systems.

(v) **Interactive Voice recognition and Response**: means a technology that usually prompts for the caller to provide information either verbally or manually to enable routing or responding to calls (the "**IVR**").

(vi) **Authenticator**: this module is a two-factor mobile authentication system to enable access to online services, using a one-time password delivered via SMS to a mobile handset.

[redacted]

(vii) **StaffMatch**: this module is an automated shift fulfilment system which enables staff registration of skills, work preferences and mobile phone numbers; integration with the Buyer's intranet or other systems, e.g. payroll, HR and setting business rules to make placement offers to casual staff members; reporting with insight on staff and management behavioural information.

(viii) **Reminder**: this module provides the ability to deliver SMS appointment and event reminders, confirm appointment attendance and report on attendance in real-time.

(ix) **StaffSafe**: this is a job dispatch and status/safety system module, which can be integrated into existing workforce management IT systems and which enables simple, automated SMS field staff check-ins, real-time safety status updates and automatic escalation.

(x) **Rapid Alert**: this module gives the Buyer the tools to quickly send template Messages to pre-defined groups of End Recipients by using the Buyer Portal to notify the Buyer's people of emergency incidents so they can respond quickly.

(xi) **Simple Template Messaging**: this module allows Administrators to create pre-defined templates that are ready for use by other Users with certain editable fields, to help eliminate potential communications errors.

(xii) **Conversational AI**: this is a license, customisation and implementation service package that enables the Buyer to deliver AI-powered chatbot, robotic process automation (RPA), live chat and virtual assistant solutions over multiple channels. The Supplier will provide the Buyer with the applicable Conversational AI service plan(s), add-on(s) and implementation package(s) set out in a separate statement of work.

Conversational AI service channels:

- SMS;
- RCS;
- WhatsApp;
- Push Notifications;
- Email;
- Facebook Messenger;
- Website – Widget;
- Website – Embedded;
- Website – Full Page; and
- any additional channels added as service options in the future as may be notified to the Buyer by the Supplier

(collectively known as "**Channels**")

(xiii) **IP Filtering**: this module provides an extra level of authentication for API calls by authenticating against the username, the password and the IP address that the API call is made from.

(xiv) **2FA for Buyer Portal**: this module allows Administrators to enable two-factor authentication for Buyer Portal users by sending one-time passwords via SMS.

(xv) **Connect API – SMS**: an API that allows the Buyer to send, receive, query or cancel SMS Messages, with records of all Messages sent via the Connect API interface recorded by the Service.

(xvi) **Omni-Channel**: this module allows the Buyer to send Messages via the Buyer Portal with multiple content types such as plain text, rich text, or voice to one or many persons (contacts, groups, lists or any specified mobile or email addresses) via multiple channels of communication such as SMS, voice, and email.

[redacted]

(xvii) **Escalations**: this module enhances the Omni-Channel Messages using either User-defined rules or rules defined by the Buyer's organisation to resend or try alternate delivery methods to increase the likelihood the Message is received and actioned.

(xviii) **Voice**: this is a voice Message broadcasting and alerting tool which allows the Buyer to create, and record spoken Messages, or input text, which are then converted to voice and broadcasted to a single mobile or landline user, or to large groups of both mobile and landline users.

(xix) **Voice API**: this module is an API interface that sends voice Messages through file attachments, text-to-speech functionality or by invoking action-based objects stored on the Buyer Portal. Action-based objects allow to combine audio-streaming, text-to-speech and pin input options in a single voice call.

(xx) **Rich Communications Services (RCS) Business Messaging**: this module allows the Buyer to create RCS Messages using the drag and drop editor and send RCS Messages to RCS-enabled devices.

(xxi) **Connect API - RCS**: this module is an API that can be used to send, receive, query or cancel RCS Messages, with a record of all Messages sent via the Connect API interface recorded in the Service.

(xxii) **Emailer**: this is an easy-to-use email campaign management tool with broadcast delivery feature for communicating with large number of recipients using email Messages, with features such as mail merge, delivery rate controls and unsubscribe controls for spam compliance.

(xxiii) **Connect API – Email**: this is an API that can be used to send, receive, query or cancel email Messages, with a record of all Messages sent via the Connect API interface recorded in the Service.

(xxiv) **High Availability (API traffic)**: this module provides an automatic failover to a second and independent instance to provide transparent failover for API traffic (only).

(xxv) **Active Directory (LDAP) Plug-In**: this module plugin allows the Buyer to sync their organisation's employee directory into a Buyer Portal's address book directly whilst reducing time and errors caused by manual updates.

(xxvi) **Shorten URL**: this module allows the Buyer to automatically convert lengthy URLs in SMS Messages to be short, branded URLs with unique ID.

(b) **Reporting and Administration Features**

(i) **Reports**: this module provides an online view of usage and messaging interactions, which can be requested by the User on an ad-hoc basis.

(ii) **Summary Reports**: this module is a separate cost centre/usage report in a predefined format, which is scheduled to be delivered to the Buyer at a pre-defined time.

(iii) **Reports+**: this module gives the Buyer the flexibility to run ad-hoc or scheduled reports for outbound Messages and inbound Messages and these reports can also be exported for processing by other systems.

(iv) **Admin+**: this module adds additional functionality by allowing the Administrator to see and manage the overall organisation hierarchy.

(v) **Content Masking Licence**: depending on the classification of data the Buyer and the Buyer's Users send in Messages, the Buyer may wish to add this module which enables the Buyer's Users to provision a licence so as to mask the content of any Messages transmitted, so that Message content is not visible in reports and cannot be extracted from the Buyer Portal.

[redacted]

(c) **Technology Options**

(i) **Basic APIs**: the basic APIs available include HTTP/S, SMTP, FTP, SMPP, REST, and WSDL, which provide the capability to integrate the Service into a variety of IT systems and customer backend systems, applications and websites.

(ii) **SSH File Transfer Protocol (SFTP)**: this module provides file access and file transfer securely from third party systems to the Buyer Portal.

(iii) **Open Secure Socket Layer (OpenSSL)**: this is an open certificate management tool that utilises Secure Socket Layer (SSL) and Transport Security Layer (TLS) to secure the Buyer's data between third party systems and the Buyer Portal using a public and private key combination.

(iv) **Virtual Private Network (VPN)**: this module secures the Buyer's data between third party systems and the Buyer Portal in its own private network by establishing a virtual point-to-point connection.

(d) **Connectivity Options**

(i) **Virtual Mobile Numbers**: the Buyer can purchase dedicated virtual mobile numbers, which can be used to receive inbound SMS Messages from End Recipients which are then forwarded to the Buyer Portal.

(ii) **Dedicated Short Codes**: the Buyer can purchase one or more dedicated Short Codes, which the Buyer can use to run messaging campaigns. End Recipients who respond to a SMS using the dedicated Short Code are charged at their Network Operator's standard SMS rate.

(iii) **Dedicated Short Codes – Free to End User**: the Buyer can purchase one or more dedicated Short Code that are free to the End Recipient, which the Buyer can use to run messaging campaigns. End Recipients who respond to a SMS using the dedicated Short Code are not charged as their SMS reply is free. Instead, the Buyer will pay the cost of the reply SMS based on the rate specified in the Price Card.

(iv) **Shared Short Codes**: the Buyer is allocated a shared Short Code which can also be used by one or more of the other Supplier customers or applications, in which case, keywords are used to identify the Buyer's business to the intended End Recipient.

(v) **Keywords**: Keywords are used with Short Codes or a dedicated virtual mobile number so that End Recipients can respond to specific adverts or campaigns. Keywords can be purchased (subject to availability) for better brand recognition.

(vi) **Alpha Tags**: the Buyer can use one or more Alphanumeric Codes or Alpha Tags to personalise the sender's name in any Messages the Buyer sends using the Service (in place of a standard mobile phone number), so the End Recipient can see the name of the brand, company or department sending the Message.

(e) **Additional Support Options**

(i) **Enhanced Support Service**: 24 x 7 x 365 direct access to the Supplier's Service Desk for technical and customer account support.

(ii) **Pre and Post Sales Technical Support**: technical support for API and other integrations.

(iii) **Professional Services**: any Professional Services in addition to the standard delivery of the Service provided by the Supplier in accordance with Paragraph 2.1.

[redacted]

(iv) **Bespoke Training**: any agreed additional training the Buyer may require as part of the Buyer's use of the Service.

(v) **Bespoke Development**: any agreed bespoke development the Buyer requires as part of the Buyer's use of the Service.

(f) The Supplier does not guarantee that the Dedicated Short Codes – Free to End User Ancillary Service will be available on all or any UK mobile virtual network operators.

1. Service Management Boundary

1.1. The Supplier will provide and manage the Service in accordance with this Call-Off Contract:

(a) commencing at the point at which a Message is submitted to the Buyer Portal and ending when there is a successful Message Delivery; and

(b) with respect to Conversational AI within the Supplier's cloud-based chatbot infrastructure, messaging and data analysis platform, excluding any Third-Party Channels.

1.2. The Supplier will have no responsibility for the Service outside the Service Management Boundary.

1.3. Subject to Paragraph 1.1 above, the Service does not include the actual delivery of a Message to the End Recipient and the Supplier will not be responsible for any failure of, or delay in, the delivery of a Message to an End Recipient provided that Message Delivery has taken place.

1.4. The Supplier does not make any representations, whether express or implied, about whether the Service will operate in combination with any Buyer equipment or other equipment and software.

1.5. Access to the Service is dependent on the suitability of any Buyer equipment (including smart phones, tablets and other similar devices capable of connecting to the internet) and, if applicable, the Buyer's network. The Buyer is responsible for the Buyer's systems, Buyer equipment, the Buyer's network and any connectivity used in connection with the Service.

1.6. It is the Buyer's responsibility to satisfy itself that the Ancillary Services the Buyer selects are suitable for the Buyer's intended purpose and requirements.

1.7. The Supplier will not be responsible in any way for any electronic communications services provided by any other Communications Provider and the Buyer is responsible for making applications to such providers, for compliance with their terms and for payment of any charges.

1.8. The Supplier is not responsible for and makes no representation or warranty for:

(a) use of the Conversational AI Ancillary Service by the Buyer's Users;

(b) use of the Buyer Data with the Conversational AI Ancillary Service; or

(c) the consequences of the Buyer's failure to fulfil any of the responsibilities stated in Paragraph 19.1.

2. Service Delivery: Supplier's Obligations

2.1. Before the Service Availability Date and, where applicable, throughout the provision of the Service, the Supplier:

(a) will provide the Buyer with contact details for the Service Desk, which will be available during Working Hours;

[redacted]

(b) will comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at any Site(s) to which the Supplier needs access in order to provide the Service and that the Buyer has notified to the Supplier in writing, but the Supplier shall have no responsibility to the Buyer if, as a result of any such compliance, the Supplier is in breach of any of its obligations under the Call-Off Contract;

(c) will provide the Buyer with an estimated date for the Service Availability Date and will use reasonable endeavours to meet the estimated Service Availability Date, but will have no responsibility for a failure to do so;

(d) may refuse to provide the Service to the Buyer for reasons of health, safety or technical compatibility where the Supplier has reason to doubt the integrity or suitability of the Buyer equipment; and

(e) provide any Professional Services as agreed between both Parties in the Order Form to support provision of the Service for the Buyer's use.

2.2. If the Buyer requests a change to the Service or any part of the Service, the Supplier may revise the Customer Committed Date to accommodate that change.

2.3. The Supplier may expedite delivery of the Service for operational reasons or in response to a request from the Buyer, but this will not revise the Customer Committed Date.

3. Commissioning of the Service

3.1. The Supplier will commission the Service during Working Hours on Working Days. Before the Service commencement, the Supplier will:

(a) configure the Service;

(b) conduct a series of standard tests on the Service to ensure that it is configured correctly;

(c) on the date that the Supplier has completed the activities in this Paragraph 3.1, confirm to the Buyer the Service Availability Date.

4. Provision of the Services

4.1. On and from the Service Availability Date, the Supplier:

(a) will maintain the Buyer Portal to provide the Buyer with online access to the Service and its functionalities;

(b) will work with relevant suppliers to restore service as soon as practicable during Working Hours if the Buyer reports an Incident to the Service Desk;

(c) may carry out Maintenance from time to time and will inform the Buyer with at least 7 days' advance notice before any planned Maintenance on the Supplier network or Supplier Equipment, however, the Supplier may inform the Buyer with less notice than normal where Maintenance is required in an emergency;

(d) may, in the event of a security breach affecting the Service, require the Buyer and the Buyer's Users to change any or all of the Buyer's User Security Details;

(e) will measure the Buyer's UK Mobile SMS Achieved Figure as at the Spend Measurement Date against the Buyer's UK Mobile SMS Committed Volume to calculate the Achieved UK Mobile SMS Usage Charges or any Underachievement Charges that are due (as applicable), where the UK Mobile SMS Commitment Option applies to the Service;

(f) may by notice to the Buyer, from time to time, specify reasonable restrictions on the volume or frequency of Messages that can be sent using the Service (designed to ensure the Supplier network is not overloaded) and the Supplier will not be responsible for any failure of Messages sent in excess or outside of such restrictions;

[redacted]

(g) to the extent permitted by Law, may access, review, monitor, audit, preserve, intercept, remove and disclose the Buyer's use of the Service and any Buyer Data, Message content or Messages (whether or not transmitted) for the purpose of:

(i) ensuring and enforcing the Buyer's compliance with the Call-Off Contract;

(ii) investigating and preventing actual or potential fraud, abuse, misconduct or other potentially unlawful behaviour;

(iii) investigating complaints received by End Recipients of Messages or other third parties;

(iv) protecting the rights or property of the Supplier (including the operation and security of the Supplier network); or

(v) complying with any Regulatory Body or Network Operator inquiries or requirements;

(h) may, without responsibility to the Buyer, limit or suspend the Buyer's access or any or all User's access to any relevant part, or where necessary all, of the Service immediately without notice:

(i) if the Supplier has reasonable cause to suspect fraudulent use of the Buyer's account(s) or sub-account(s) or breach or suspected breach of an operator or regulator's code of practice; or

(ii) upon instruction by emergency services, any Network Operator, any Regulatory Body or other appropriate authority;

(i) may from time-to-time quality check the installation of any Buyer equipment to ensure that it meets the requirements of the Call-Off Contract and all applicable health and safety and other relevant requirements; and

(j) may disconnect any Buyer equipment without prior notice to the Buyer, should a fault occur that is considered by the Supplier to affect or be likely to affect the performance of the Supplier network or the Service.

4.2. The Supplier will use reasonable endeavours to provide the Buyer with an uninterrupted Service where technically possible, but the Buyer understands that:

(a) from time-to-time Incidents may occur;

(b) the quality and availability of the Service is subject to factors beyond the Supplier's control, including:

(i) local geography and topography;

(ii) weather or atmospheric conditions;

(iii) degradation, congestion or maintenance requirements of the Supplier network including but not limited to re-positioning or decommissioning of mobile base stations;

(iv) other physical or electromagnetic obstructions or interference;

(v) faults in, or availability of, other telecommunications networks to which the Supplier network is connected;

(vi) acts or omissions of any other Providers to which the Supplier network is connected; and

(vii) the compatibility of any Buyer equipment the Buyer uses.

[redacted]

(c) the Service platform does not provide data encryption capabilities at rest and the Supplier will not be responsible for any loss or corruption of any data;

(d) the Supplier does not guarantee that it will be able to remedy all Incidents the Buyer reports or that the Supplier will be able to advise on all Service-related issues;

(e) the Supplier does not guarantee the security of the Service against unauthorised or unlawful access or use; and

(f) the Supplier will not be responsible for any failures in the supported applications and operating systems that cannot be resolved using the Service, or for the Buyer's failure to correctly follow the Supplier's advice and recommendations.

4.3. Where the Buyer has a compatibility or interface requirements, the Buyer will ensure that any elements of the Buyer Software, Buyer equipment or Buyer Assets to which the Services must interface or be compatible with are confirmed to the Supplier prior to the acceptance of the Order and all such elements will be recorded on the Order Form to enable the Supplier to assess the impact of such compatibility requirements on the Service and the associated Charges. The Buyer will provide any additional information reasonably requested by the Supplier in relation to the Buyer Software, Buyer equipment or Buyer Assets.

4.4. Notice in relation to new releases of Software used by the Supplier as part of the Service will not be provided. In the case of any material errors in the Software that become apparent in the course of operation, the Supplier will be entitled to correct those errors in future releases of the Software.

4.5. Notice may not be provided to the Buyer in relation to emergency Maintenance.

5. Access to Emergency Services

5.1. The Service does not provide the ability for Users to call the emergency services by dialling "999" or "112" and the Buyer will make alternative arrangements for Users.

6. Change

6.1. To enable the Buyer to access the Supplier's online change control systems, the Supplier's standard change control documentation will supplement the Variation Form required in Clause 24 of the Core Terms and Joint Schedule 2 (Variation Form).

6.2. Any changes to the Buyer's tariff introduced by a Variation will take effect from the next billing date provided the change is agreed by the Parties more than 10 Working Days prior to that date. Where changes are agreed less than 10 Working Days prior to that date the Charges will take effect from the following billing date.

7. Intellectual Property Rights and Software

7.1. There is no Specially Written Software or New IPR provided as part of the Service. All Software used in the provision of the Services is COTS Software and will be licenced in accordance with the Call-Off Contract. Occasionally third-party software included in the Service may be licenced to the Buyer by the Supplier or by its suppliers rather than directly by the particular third-party Software vendor. The Buyer will not copy, decompile, modify or reverse engineer any Software or knowingly allow otherwise unless allowed by law or where the Supplier has given the Buyer permission in writing.

8. Licence

8.1. The Supplier grants the Buyer and the Buyer's Users the right for the term of the Call-Off Contract to access and use the Buyer Portal and the Service in accordance with the Call-Off Contract for the Buyer's own business use only.

8.2. If applicable to the Buyer's Service as specified in the Order Form where the Buyer is managing the Service for the Buyer's corporate customer(s), the Supplier grants the Buyer the right to

[redacted]

provide access to the Buyer Portal and the Service in accordance with the Call-Off Contract to the Buyer's corporate customer(s) for their own business use only.

8.3. If requested by the Supplier, the Buyer will provide written confirmation that the Buyer has deleted any copies of the Software that the Buyer has downloaded to the Buyer's systems and the passwords used to access the Software.

8.4. The Supplier will provide the Buyer with copies of the Guidance Documentation (via the Buyer Portal) and grant to the Buyer a non-exclusive and non-transferable right to copy and disclose the Guidance Documentation for the Buyer, and where not otherwise expressly restricted, the Buyer's Users' use of the Service.

8.5. If the Buyer provides any designs or specifications for modification of the Conversational AI Ancillary Service, regardless of whether the Buyer has paid additional Charges to do so, and unless otherwise specified in writing in a statement of work:

(a) the Intellectual Property Rights in any modified system shall belong to the Supplier or its relevant third party supplier and the Buyer hereby assigns any and all rights that the Buyer may have to the same to the Supplier or its third party supplier, and waive or shall procure the waiver of any and all moral rights in the same; and

(b) the Buyer warrants that the use of those designs or specifications for the modification shall not infringe the rights of any third party.

9. Environmental Requirements

9.1. If the Buyer requires the Supplier to comply with a Buyer-specific Environmental Policy when working on a Buyer's Site, the Buyer will provide a copy of that Environmental Policy prior to placing an Order.

10. Security Requirements

10.1. It is agreed between the Parties that Part A of Call-Off Schedule 9 (Security) applies, and the Supplier's Security Management Plan will be appended to the Order Form.

10.2. In the event that Supplier Staff do not have the necessary clearance required under Call-Off Schedule 18 (Background Checks), the Parties will agree an acceptable alternative such as escorted access.

11. Personnel

11.1. Optional sections Parts A, B & D of Call-Off Schedule 2 shall not apply to this Service Offer, a transfer on service commencement is not envisaged. Part C shall apply to the Service Offer. The Supplier has made no provision for a staff transfer. For clarity, the requirement to provide information in accordance with Call - Off Schedule 2 Part E is limited to the provision of the information only in relation to any Supplier Staff who are organised to and wholly or mainly engaged in provision of the Services at Exit.

11.2. It is assumed that Supplier Staff are not required to enter into a direct confidentiality agreement with the Buyer as the Supplier will procure the compliance of Supplier Staff with the applicable confidentiality obligations in the Call-Off Contract.

12. Resale

12.1. The Buyer will not re-sell the Services to a third party without the Supplier's prior written approval or unless explicitly set out in this Service Offer. If the Supplier grants such approval, it will be conditional upon the Buyer imposing on the relevant third party in writing obligations no less onerous than those to which the Buyer is subject under this Call-Off Contract and Service Offer.

13. BCDR

13.1. The Parties agree that this Call-Off Contract has not been specified as a Critical Service Contract under Call-Off Schedule 8 (Business Continuity and Disaster Recovery).

[redacted]

14. Publicity

14.1. The Buyer consents to internal marketing by the Supplier to inform its employees that the Order has been placed, of the name of the Buyer, of the nature of the proposed services and of the value of the business to the Supplier. If the Buyer does not wish to allow such internal marketing, it is requested to notify the Supplier in writing prior to the acceptance of the Order.

15. Service Transition

15.1. If the Buyer is transitioning its existing services to the Supplier, the Buyer will provide any information or access the Supplier reasonably requests including:

(a) an inventory list with information relating to each service to be transitioned with relevant specifications, including, where applicable:

(i) the location of the service.

(ii) Software licence information;

(iii) network diagrams;

(iv) details of any third-party contracts, service level agreements and equipment;

(v) copies of relevant extracts of the Buyer's supplier support contracts for the services that are to be transitioned.

15.2. It is assumed the existing service level agreements with the Buyer's previous supplier remain the same as set out in any documents provided to the Supplier, unless the Buyer provides the Supplier notice.

16. Associated Services and Third Parties

16.1. The Buyer will need an internet connection to enable the Buyer's access and use of the Service, including any Buyer equipment necessary for such internet connection. Such internet connection may be provided by the Supplier (under a separate contract) or by another Communications Provider.

16.2. The Supplier will not be responsible for failure to or delay in supplying the Service if another supplier delays or refuses the supply of an electronic communications service to the Supplier and no alternative service is available at reasonable cost.

16.3. The Service may interface with websites, communication channels, and applications made available by third parties, including without limitation the Channels, ("**Third Party Channels**"). The Buyer acknowledges that use of such Third-Party Channels by the Buyer or the Users is solely at the Buyer's/their own risk, and the Supplier makes no recommendation, representation, warranty or commitment and shall have no responsibility to the Buyer, or obligation whatsoever in relation to them. Use of the Third-Party Channels is subject to their terms and conditions. The Supplier is not responsible for the provision of the Third-Party Channels or for any software, middleware or platform other than the Service.

16.4. Any open-sourced software provided as part of the Conversational AI Ancillary Service will be specified in the relevant statement of work and may only be used according to the terms and conditions of the specific licence under which it is distributed.

17. Service Delivery: Buyer's Obligations

17.1. The Buyer will:

(a) provide the Supplier with all relevant information in relation to health and safety and the environment as well as any other information and materials as the Supplier may reasonably request in order to provide the Services and will ensure that such information is accurate and complete in all material respects;

[redacted]

(b) provide reasonable assistance to and comply with reasonable requests from the Supplier relating to the Services;

(c) complete any preparation activities that the Supplier may request to enable the Buyer to receive the Service promptly and in accordance with any reasonable timescales;

(d) be responsible for the Buyer's usage of the Service, whether or not the Supplier has applied any usage limit or is able to advise the Buyer at any particular time if the Buyer has exceeded any applicable usage limit;

(e) provide the Supplier with the names and contact details for the Buyer Authorised Representative, but the Supplier may also accept instructions from a person who the Supplier reasonably believes is acting with the Buyer's authority;

(f) inform the Supplier promptly of any changes to the Buyer Authorised Representative or the Administrator or their contact details;

(g) provide the Supplier with any information or assistance reasonably required without undue delay, including to verify the Buyer's compliance with the Buyer's obligations under the Call-Off Contract and to enable the Supplier to comply with all requests, requirements and conditions imposed on the Supplier under applicable Law or by any Network Operator or Regulatory Body in connection with the Service;

(h) where required, provide the Supplier with access to any Site(s) during Working Hours, or as otherwise agreed, to enable the Supplier to set up, deliver and manage the Service;

(i) provide the Supplier with notice of any health and safety rules and regulations and security requirements that apply at the Site(s) where access to such Sites(s) is required;

(j) ensure, at the Buyer's own expense, the integrity and suitability of any Buyer equipment the Supplier is asked to provide the Service on, to or interface with;

(k) with respect to the Conversational AI Ancillary Service:

(i) provide all relevant data & information to enable the deployment of the Ancillary Service;

(ii) be responsible for setting, testing and signing off any logic driving the Messages to be sent to End Recipients and content of the Messages, and the Supplier shall have no responsibility with respect to any loss or damage suffered by the Buyer or a third party as a result of such logic and content, and

(iii) be responsible for ensuring the End Recipient is aware of the use of the Conversational AI Ancillary Service;

(l) for Sites not under the Supplier's control, obtain and maintain all necessary consents, licences, permissions and authorisations that are required for the provision of the Services to the Buyer at the Sites including consents for alterations to buildings or entrance to property required from local authorities, landlords or owners for:

(i) the installation of Supplier Equipment or Purchased Equipment; or

(ii) the use of the Services over the Buyer's network or at a Site.

17.2. The Buyer shall not:

(a) make any unauthorised alteration or modification of any Services; or

(b) use of any Services in conjunction or combination with other equipment or software or any other services not supplied by the Supplier.

18. Service Operation

18.1. The Buyer will:

[redacted]

(a) ensure that Users report Incidents to the Buyer Authorised Representative and not to the Service Desk;

(b) ensure that the Buyer Authorised Representative takes Incident reports from Users and passes these to the Service Desk using the reporting procedures agreed between both Parties, and is available for all subsequent Incident management communications;

(c) be responsible, at the Buyer's sole cost, for:

(i) the supply, monitoring and maintenance of any Buyer equipment (including software updates) connected to or used in connection with the Service; and

(ii) any loss the Supplier suffers as a result of the Buyer equipment causing a fault on the Supplier network, including the costs of rectification;

(d) ensure that any Buyer equipment that is connected to the Service or that the Buyer uses, directly or indirectly, in relation to the Service is:

(i) connected using the applicable network termination point, unless the Buyer has the Supplier's permission to connect by another means;

(ii) adequately protected against viruses and other breaches of security;

(iii) in conformance with the interface specifications and routing protocols specified by the Supplier;

(iv) technically compatible with the Service and will not harm or damage the Supplier Equipment, the Supplier's network, or any of the Supplier's suppliers' or subcontractors' network or equipment;

(e) immediately remove or disconnect any Buyer equipment, or advise the Supplier to do so at the Buyer's expense, where Buyer equipment does not meet any relevant instructions, standards or applicable Law; and redress the issues with the Buyer equipment prior to reconnection to the Service;

(f) implement adequate measures for the purpose of monitoring and preventing fraudulent use of the Buyer's account and the Service;

(g) where applicable, ensure the confidentiality, security and proper use of all valid User Security Details, access profiles, passwords and other systems administration information used in connection with the Service and:

(i) as soon as reasonably practicable terminate access for any person who is no longer a User;

(ii) inform the Supplier immediately if a User's ID or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;

(iii) inform the Supplier immediately if the Buyer becomes aware of any suspected or actual breach of security or unauthorised use of the Service, the Messages or any User Security Details and the Buyer will remain responsible for all Charges incurred by the unauthorised use of the Buyer's account(s) and subaccount(s) until the Supplier restricts or bars the relevant account(s) or sub-account(s);

(iv) take reasonable steps to prevent unauthorised access to the Service;

(v) satisfy the Supplier's security checks if a password is lost or forgotten; and

(vi) change any or all passwords or other systems administration information used in connection with the Service if the Supplier requests the Buyer to do so in order to ensure the security or integrity of the Service or where there has been a security breach affecting the Service;

[redacted]

(h) where applicable, distribute, manage and maintain User Security Details, access profiles, passwords and other systems administration information relating to the control of Users' access to the Service;

(i) where applicable, maintain a list of current Users and provide a copy of such list to the Supplier within five Working Days following the Supplier's written request at any time;

(j) ensure that the maximum number of Users will not exceed the permitted number of User identities as set out in any applicable Order Form;

(k) not allow any User specific subscription to be used by more than one individual User unless it has been reassigned in its entirety to another individual User, in which case the Buyer will ensure the prior User will no longer have any right to access or use the Service;

(l) ensure all Messages sent by the Buyer and the Buyer's Users will:

(i) include a source indication within each Message (i.e. mobile phone telephone number, "From" field in the Message, etc);

(ii) be of a type which is capable of being retained by the End Recipient;

(iii) not specify any expiry period for undelivered Messages in excess of three days from the date when a Message is submitted for delivery;

(iv) comply with any requirements under applicable Law to enable the End Recipient to opt out of receiving Messages; and

(v) not cause an End Recipient to be misled as to the originator of a Message, including misleading the End Recipient into believing that the originator of a Message is the Supplier or any Supplier Affiliate or is connected with or authorised by the Supplier or any Supplier Affiliate;

(m) comply with:

(i) any reasonable directions of the Supplier resulting from directions made by a Network Operator or any Regulatory Body in relation to the Buyer Data, the Messages or the Service;

(ii) any relevant code of practice and guidelines issued under applicable Laws and any industry code of practice (including marketing and advertising industry guidelines) adopted by the Supplier in relation to the Service and notified by the Supplier to the Buyer from time to time; and

(iii) all manuals, guidance and reasonable instructions the Supplier issues to the Buyer regarding the use of the Service or the Supplier network and the Supplier's reasonable security and other checks relating to access or use of the Service;

(n) ensure that before any Message is sent or Buyer Data or other material (whether proprietary or non-proprietary) is used as part of the Service:

(i) all requisite rights, licences, permits, authorisations, certifications and consents have been obtained and maintained throughout the term of the Call-Off Contract;

(ii) it does not infringe the Intellectual Property Rights or other rights of any person; and

(iii) all requirements of applicable Law are complied with,

and the Supplier may request evidence of the Buyer's compliance with this Paragraph and the Buyer will promptly comply with such request;

(o) comply with any notice from the Supplier in accordance with Paragraph 4.1(f) above specifying any reasonable restrictions and instructions on the volume or frequency of Messages that can be sent using the Service; and

(p) notify the Supplier immediately if:

[redacted]

(i) the Buyer becomes aware of or suspects the Service is being used for any unlawful, fraudulent or improper purposes or in any way that may expose the Supplier or its suppliers to the risk of any legal or administrative action, including prosecution under any applicable Law;

(ii) the Buyer becomes aware of any allegation that any Buyer Data may infringe applicable Law or infringe any third-party Intellectual Property Rights; and

(iii) any third party makes or threatens any Claim against the Buyer, the Supplier, any Supplier Affiliate or any other party relating to any Buyer Data, any Message or the Service.

(q) warrant and represent to the Supplier that:

(i) the Buyer will only use the Service (or permit Users to use the Service) to send Messages to End Recipients that have duly consented or "opted-in", as required by Data Protection Legislation, to:

- receiving the quantity, frequency and types of Messages sent; and
- their Personal Data being used to in relation to the Service; and

(ii) such consents or opt-ins have not been withdrawn.

(r) operate an effective system for End Recipients to exercise their rights not to receive Messages under relevant Data Protection Legislation and will comply with any reasonable instructions issued by the Supplier in relation to such system;

(s) on receiving a written request from the Supplier, promptly provide the Supplier with proof of End Recipient opt-in requests, opt-out requests, and the Buyer's response time for discontinuing the provision of Messages to those End Recipients that have opted-out, to the Supplier's satisfaction;

(t) acknowledge that the Supplier or its suppliers may temporarily or permanently opt-out one or more of the End Recipients or any of their personal contact details at any time for any reason, including if the Supplier receives a request to "opt-out" received from the End Recipient directly or a Network Operator. The Buyer will not re- "opt-in" an End Recipient unless they subsequently agree to receive communications from the Buyer;

(u) be solely responsible for the Buyer's relationship (contractual or otherwise) with End Recipients including, where applicable, communicating pricing information to them.

18.2. The Supplier shall use a supported version of anti-virus Software available from an industry accepted anti-virus Software vendor.

18.3. If the Buyer is required under the Order to provide information, assistance, or access to the Supplier to comply with the Supplier's instructions, the Buyer will provide the same cooperation to EE Ltd for delivery of the Service.

19. Use of Service

19.1. The Buyer will not and will ensure that the Buyer's Users will not:

(a) re-sell, transfer, assign or sub-licence the Service (or any part of it) or the associated Software to anyone else;

(b) modify, reverse engineer or make derivative works of any Software provided under the Call-Off Contract, or knowingly let anyone else do that, unless it is allowed by applicable Law or the Supplier has given the Buyer permission in writing;

(c) interfere with or disrupt the integrity or performance of the Software or its data;

(d) attempt to gain unauthorised access to the Software or its related systems or networks; or

(e) use the Service or knowingly allow the Service to be used:

[redacted]

(i) for any unlawful, fraudulent or improper purposes or in any way that may expose the Supplier or its suppliers to the risk of any legal or administrative action, including prosecution under any applicable Law;

(ii) in any way that may impair the integrity or operation of the Buyer Portal, the Supplier network, the Software, the network, systems or software of any Providers or the Supplier's provision of the Service to the Buyer or other customers and Users;

(iii) in a manner that materially interferes with the use of the Supplier's platform by other customers, uses any artificial inflation of service or denial of service means, or exceeds the maximum throughput allocated to the Buyer's account, or to reverse-engineer or copy any portion of any of the Supplier's service process, methodology, code or program;

(iv) to send or store any Message, communication or material which:

- is false, misleading, obscene, indecent, threatening, offensive, abusive, discriminatory, defamatory, libellous or otherwise unlawful or tortuous;
- is or may be harmful to children in any way;
- causes any nuisance, annoyance, inconvenience or needless anxiety (as set out in the Communications Act 2003);
- is spam, duplicative or is otherwise unsolicited in violation of applicable Laws;
- violates any Regulatory Body or Network Operator requirements or codes of practice;
- violates the Intellectual Property Rights or privacy rights of the Supplier, any Supplier Affiliate or any third party;
- contains software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs;
- contains malware that could reasonably be considered obscene, defamatory, offensive.

19.2. The Buyer will be solely responsible for:

(a) all Messages, communications and materials sent or stored using the Buyer's or the Buyer's Users' account(s) and sub-account(s);

(b) all activities that occur on or through use of the Buyer's or the Buyer's Users' account(s) and sub-account(s) for the Service, whether authorised by the Buyer or not; and

(c) the acts, omissions or breaches of the Buyer's Users with respect to their use of the Service and compliance with this Call-Off Contract.

20. Alphanumeric Codes, Short Codes and APIs

20.1. The Buyer will follow any reasonable process the Supplier notifies the Buyer of prior to using any Alphanumeric Codes and the Supplier may require the Buyer at any time to cease using a particular Alphanumeric Code.

20.2. The Buyer will ensure that all Alphanumeric Codes the Buyer uses:

(a) do not mislead the End Recipient as to the originator of the Message;

(b) do not imply any connection with the Supplier or any Supplier Affiliate, whether by use of the Supplier's name or the Supplier's strap line or other Supplier branding tool (or part thereof);

(c) are not offensive, obscene or unlawful; and

(d) comply with all relevant codes of practice.

[redacted]

20.3. Any Short Codes allocated to the Buyer and used by the Buyer will remain at all times the property of and subject to the applicable terms and conditions imposed by the entity authorised to administer such Short Codes and all Short Codes are non-transferable. At the Buyer's request in any applicable Order Form and subject to availability, the Supplier may allocate Short Codes to be used by the Buyer as part of the Service. All Short Codes (dedicated or shared) are subject to a minimum three-month termination notice period. The Buyer's rights to use any Short Codes will cease on termination of the Service.

20.4. Ownership of any APIs provided by the Supplier or its suppliers will remain vested in the Supplier or its supplier(s). The Buyer will be permitted to use such APIs so long as the Buyer complies in all material respects with the Call-Off Contract and continues to pay the Charges for such APIs. The Buyer's rights to use any APIs will cease on termination of the Service.

21. Buyer Data

21.1. Depending on the Ancillary Services the Buyer selects, the Supplier may provide the Buyer with the means of uploading and storing Buyer Data via the Buyer Portal.

21.2. The Supplier will not be under any obligation to store Buyer Data and the Supplier will not have any responsibility if any stored Buyer Data is deleted, destroyed, damaged, or lost either during normal operation or in the event of an Incident with the Service.

21.3. The Buyer will be solely responsible for the quality, accuracy, integrity, legality, appropriateness, and intellectual property ownership or right to use the Buyer Data and the content of any Messages sent by or on the Buyer's behalf.

21.4. The Supplier recommends that the Buyer classifies any Message content or Buyer Personal Data when using the Service platform and that the Buyer saves and archives back-up copies of any Buyer Data on the Buyer's own devices and platforms not connected with the Service.

21.5. The Buyer grants (or will procure the grant) to the Supplier and its supplier's permission for the term of the Call-Off Contract to use the Buyer Data to the extent necessary to deliver the Service and perform its obligations under the Call-Off Contract. By submitting and sending Buyer Data through use of the Service, the Buyer grants the Supplier and its supplier's permission to store, process and transmit the Buyer Data as necessary to deliver the Service and perform its obligations under the Call-Off Contract. In order to deliver the Service, the Supplier and its suppliers may need to modify the Buyer Data as necessary to meet any requirements or limitations of any Network Operators, devices, services or media.

21.6. Buyer Data may be used by the Buyer for the Conversational AI Ancillary Service to assist with continuous improvements in providing that Service to the Buyer.

22. Service Amendments

22.1. As part of the Supplier's continuous improvement programme, it may make any minor amendment to the Smart Messaging (Tailored Service) Service that does not have an adverse effect on the performance or provision of a Service.

23. Charges and Payments

23.1. Where invoices are issued online, the Supplier will notify the Buyer by email when a new invoice is issued.

23.2. Where the Buyer makes an aggregated payment in respect of more than one invoice:

(a) the Buyer may give the Supplier instructions about which amounts to apply to which invoices; and

(b) if the Buyer does not give instructions in accordance with Paragraph 23.2(a), the Supplier may apply any amount of the aggregated payment to any unpaid invoices at its discretion.

[redacted]

23.3. The Supplier may subcontract some or all the delivery of Services to EE Ltd and will assign the benefit of Order to EE Ltd in respect of ordering, provision, Maintenance and/or invoicing and payment for the Services.

24. Invoicing

24.1. Due to the standard nature of invoicing for these Services, the unique Order reference number may be included on each invoice if provided by the Buyer.

24.2. The Supplier will invoice the Buyer for the following Charges in the amounts set out in any applicable Order Form:

(a) Recurring Charges, monthly in arrears on the first day of the relevant month and for any period where the Service is provided for less than one month, the Recurring Charges will be calculated on a daily basis; and

(b) One-Off Charges and Usage Charges, monthly in arrears, calculated at the then current rates;

(c) channel related One-Off Charges, monthly in arrears, or before Service Availability Date, depending on the channel and where applicable;

(d) where the UK SMS Commitment Option applies, any Achieved UK Mobile SMS Usage Charges or any Underachievement Charges (as applicable), monthly in arrears.

24.3. The Supplier may invoice the Buyer for any of the following Charges in addition to those set out in any applicable Order. Charges will be calculated in accordance with the day rates set out in Table 8 in the Price Card below:

(a) Professional Service Charges, in arrears upon completion of any agreed work or as set out in any applicable Order Form, where the Buyer requires any additional work which falls outside the scope of the Service set out in this Call-Off Contract and which will be scoped and agreed with the Supplier in advance of work commencing and charged as set out in the Order Form;

(b) Charges for investigating Incidents that the Buyer reports to the Supplier where the Supplier finds no Incident or that the Incident is caused by something for which the Supplier is not responsible under the Call-Off Contract;

(c) Charges for commissioning the Service in accordance with Paragraph 3.1 outside of Working Hours;

(d) Charges for expediting provision of the Service at the Buyer's request after the Supplier has informed the Buyer of the Customer Committed Date;

(e) Charges for changes to a Service prior to the Service Availability Date because the Buyer has given the Supplier incomplete or inaccurate information; and

(f) Charges incurred, up and until the Buyer informs the Supplier, from the unauthorised use of the Buyer's accounts and/or subaccount(s).

24.4. All Charges will be calculated in accordance with details recorded by, or on behalf of, the Supplier.

25. COTS Software Licence Terms and Terms of Service

25.1. The Supplier will only provide the Service if, where applicable, the Buyer has entered into the End User Licence Agreements with the Supply Chain and the suppliers of the Channels the Buyer is using, as may be amended or supplemented from time to time ("**EULA**").

25.2. The Buyer will observe and comply with the EULA for all and any use of the applicable Software & Channels.

[redacted]

25.3. The Buyer will enter into the EULAs for the Buyer's own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULAs are between the Buyer and the relevant Channel suppliers and the Buyer will deal with the relevant Channel suppliers with respect to any loss or damage suffered by either of them as such loss or damage will not be enforceable against the Supplier.

25.4. Where the EULA is presented in a 'click to accept' function and the Buyer requires the Supplier to configure or install Software on the Buyer's behalf, the Supplier will do so as the Buyer's agent and bind the Buyer to the EULA.

25.5. If the Buyer is using the Service offered by WhatsApp Channel supplier, the Buyer is required to accept applicable WhatsApp Business Terms of Service ("**ToS**"), available at: https://www.whatsapp.com/legal/business-terms/ and as may be amended or supplemented from time to time by the Channel supplier. The Buyer acknowledges that WhatsApp Channel of the Service can only be provided by the Supplier if the Buyer has accepted the ToS.

25.6. By accepting the ToS the Buyer agrees to observe and comply with ToS and any additional terms and policies referenced in ToS for any and all use of the Service.

25.7. The Buyer accepts responsibility in accordance with the ToS for the use of the services offered by WhatsApp Channel supplier accessible through the Service.

25.8. The Buyer acknowledges that the Buyer enters into the ToS for the Buyer's own benefit and that the rights, acknowledgements, undertakings, warranties and indemnities granted under the ToS are between the Buyer and the WhatsApp Channel supplier.

25.9. Any loss or damage suffered by the Buyer or the WhatsApp Channel supplier under the ToS will be enforceable only between the Buyer and the Channel supplier and will not be enforceable against the Supplier.

25.10. If the Buyer does not comply with the EULA, Supplier may restrict the Service upon reasonable notice.

25.11. Any applicable EULA will be incorporated in an Order via Call-Off Schedule 24 (Supplier Furnished Terms).

26. Ending the Contract

26.1. Each Buyer has the right to terminate their Call-Off Contract at any time by giving the Supplier not less than the minimum period of notice specified in the Order Form. Under such circumstances the Buyer agrees to pay the Supplier's reasonable and proven unavoidable Losses resulting from termination of the Call-Off Contract, provided that the Supplier takes all reasonable steps to minimise such Losses. The Supplier will give the Customer a fully itemised list of such Losses, with supporting evidence, to support their claim for payment. After the Call-Off Contract ends Clauses 10.6.1 to 10.6.5 of the Core Terms will apply.

26.2. If the Buyer terminates the Call-Off Contract, all or part of it, for convenience prior to the end of the Contract Period, or if the Supplier terminates the Call-Off Contract the Buyer will pay the Supplier:

(a) all outstanding Charges or payments due and payable under the Call-Off Contract; and

(b) all outstanding Charges for the Service rendered.

26.3. On termination of the whole or part of the Service by either Party in accordance with the Core Terms, the Supplier:

(a) will provide configuration information relating to the Service provided at the site(s) in a format that the Supplier reasonably specifies;

(b) de-activate the Buyer's and the Buyer's Users' access to the Service;

(c) disconnect and remove any Supplier Equipment located at the Site(s) (if any);

[redacted]

(d) terminate all licenses and permissions granted to the Buyer under the Call-Off Contract with immediate effect;

(e) remove the Buyer's account(s), sub-account(s) and delete any associated Buyer Data and Content from the Buyer Portal and underlying platforms subject to the Supplier's or its suppliers' retention obligations under applicable Law;

(f) will provide reasonable assistance to the Buyer in line with standard telecommunication industry practice to transfer any part of the Service to another telecommunications provider.

26.4. On expiry or termination of the Service by either Party, the Buyer will:

(a) immediately stop using the Service, except for Supplier Software embedded in devices or equipment to which the Buyer has title:

(i) that cannot reasonably be removed or deleted from that device or equipment; and

(ii) to the extent strictly necessary for the ongoing use of that device or equipment;

(b) where such termination occurs after the end of the Call-Off Initial Period the Buyer will be refunded any Recurring Charges the Buyer has paid in advance for the remaining days left in that calendar month;

(c) immediately cease (and ensure that the Buyer's Users immediately cease) to access and use the Service;

(d) provide the Supplier with all reasonable assistance necessary to remove Supplier Equipment from the Site(s) (if any);

(e) disconnect (or assist the Supplier to disconnect) any Buyer equipment from any Supplier Equipment located at the Site(s) or the Supplier network;

(f) not dispose of or use any Supplier Equipment (if any) other than in accordance with the Supplier's written instructions or authorisation;

(g) arrange for any Supplier Equipment located at the Site(s) (if any) to be returned to the Supplier and be responsible for any reasonable costs of recovery that the Supplier incurs in recovering any Supplier Equipment.

27. Supplier Equipment

27.1. By placing an Order, the Buyer hereby approves the delivery of any Supplier Equipment and confirms that work on the Buyer Premises can commence.

27.2. Prior to the Call-Off Expiry Date the Buyer will confirm to the Supplier whether it wishes to request the re-use any Supplier Equipment following expiry (rather than the removal of that Supplier Equipment).

28. WEEE Directive

28.1. The Buyer will comply with Article 13 of the WEEE Directive for the costs of collection, treatment, recovery, recycling and environmentally sound disposal of any equipment supplied under the Call-Off Contract that has become WEEE.

28.2. For the purposes of Article 13 of the WEEE Directive this Paragraph 28 is an alternative arrangement to finance the collection, treatment, recovery, recycling and environmentally sound disposal of WEEE.

28.3. The Buyer will comply with any information recording or reporting obligations imposed by the WEEE Directive.

29. Notification of Incidents

29.1. Where the Buyer becomes aware of an Incident:

[redacted]

(a) the Buyer Authorised Representative will report it to the Service Desk;

(b) the Supplier or the Supplier's supplier will give the Buyer a Ticket;

(c) the Supplier or the Supplier's supplier will inform the Buyer when it believes the Incident is cleared and will close the Ticket when:

(i) if the Buyer confirms that the Incident is cleared within 24 hours after having been informed; or

(ii) the Supplier or the Supplier's supplier has attempted unsuccessfully to contact the Buyer and the Buyer has not responded within 24 hours following the Supplier's attempt to contact the Buyer; and

(d) the Buyer confirms that the Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and the Supplier or the Supplier's supplier will continue to work to resolve the Incident.

30. Schedules

30.1. The Services set out in this Service Offer include those standard products/services that will be provided by the Supplier. They do not include Charges for the services listed below which the Buyer may select. The Parties will need to agree any additional details for those services selected from the options below based on the Buyer's specific requirements. If any of the excluded schedules are required, a new service offer can be published that will include them:

- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties) including Annex 5 – including optional Terms for Bronze Contracts
- Joint Schedule 8 (Guarantee)
- Joint Schedule 9 (Minimum Standards of Reliability)
- Joint Schedule 12 (Supply Chain Visibility)
- Call-Off Schedule 6 (ICT Services)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery) Part B (including bronze contracts provision)
- Call-Off Schedule 9 (Security) part B
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 11 (Installation Works)
- Call-Off Schedule 12 (Clustering)
- Call-Off Schedule 13 (Implementation Plan and Testing)
- Call-Off Schedule 14 (Service Levels) other than those specified in the service offer
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 16 (Benchmarking)
- Call-Off Schedule 18 (Background Checks)
- Call-off Schedule 22 (Lease Terms)

Paragraphs 1 – 30 of this Service Offer will be construed as the content that comprises Schedule 25 (Supplier Operational Terms).

Conditions on the Buyer (Including Supplier Furnished Terms)

Not applicable.

[redacted]

Smart Messaging (Tailored Service) Outline Implementation Plan

Standard Plans

The Supplier shall implement its standard delivery plan for the delivery of the Services.

Only dates identified as Milestones in the standard delivery plan will attract Delay Payments, otherwise all dates and timescales are estimates only.

Standard Services - SMS

Pre-Sales

- The Supplier's sales consultant sets up a meeting with the Buyer to gather requirements.
- The Supplier provides a proposed solution design to the Buyer for approval, along with a request for details required for provisioning.
- Once the Buyer approves the proposal, an RM6116 Call-Off Contract Order Form is sent to the Buyer.

On-boarding process and Implementation Plan (Working Days)

Day 1	RM6116 Call-Off Contract Order Form signed by both parties.
Day 2	The Supplier completes Sales Order Request (SOR) form, for provisioning purposes.
Days 3 to 5	The Supplier's platform support provisions customers in platform following SOR instructions.
Day 6	Once provisioned an automatic welcome email is sent to the Buyer from the platform.
Day 7	The Buyer can then log in to the platform with login and password supplied.
Day 8	The Supplier will contact the Buyer and offer training.
	The Supplier to conduct training session if required.

Other Channels

The on-boarding process and Implementation Plan for other channels (including email, voice and Rich Communications Services) may vary. Implementation timelines will be clarified during pre-sales phase.

[redacted]

Smart Messaging (Tailored Service) Service Levels and Service Credits

(a) The default Service Levels in Call-Off Schedule 14 (Service Levels) are replaced by the service-specific Service Levels set out here.

(b) There are no Service Credits provided as part of this Service.

(c) There are no guaranteed Service Levels for the Service, as the quality and availability of the Service is subject to factors beyond the Supplier's control.

(d) From the Service Availability Date, the Supplier will aim to respond and resolve Incidents in accordance with the following Service Levels:

Incident Priority	Description of Incidents	Risk category	Service Desk Availability	Target Response Time	Target Resolution Time
P1 Incident	Service unavailable to many or all Users.	Very High	24 hours per day 7 days per week	1 hour	8 hours
P2 Incident	Service performance impaired or slow or delayed User functions. Many Users affected.	High	24 hours per day 7 days per week	2 hours	12 hours
P3 Incident	Service or a feature is slow or not functioning correctly. One or more Users affected.	Medium	Working Hours	1 Working Day	2 Working Days
P4 Incident	An information request such as support question.	Low	Working Hours	1 Working Day	2 Working Days

(e) The Service Levels are targets only and the Supplier will not pay compensation if it does not meet any Service Level.

(f) If the Buyer reports an Incident and the Supplier can find no fault with the Service, the Supplier may apply a Charge for any work that the Supplier undertakes.

(g) The Target Response Time and Target Resolution Times set out above will start from the time that the Incident is raised by the Buyer and a fault reference number is provided.

(h) Target Response Time or reference to 'respond' means the Supplier will aim to acknowledge the Incident by providing the Buyer with a Ticket within the times shown above.

(i) Target Resolution Time means the Supplier will aim to resolve the Incident (depending on priority or "P" level) within the times shown above.

[redacted]

Smart Messaging (Tailored Service) Price Card

Price Card version A, 1 February 2024

All prices exclude VAT.

The Service Period applicable to this Service Offer is 12 months. The Minimum Period of Service is 12 months starting from the Service Availability Date.

First time Buyers may need to order Professional Services from the Supplier where applicable, as detailed in Table 8 below. The Buyer will need to contact its BT Account Manager prior to ordering this Service. The Buyer will be asked to complete a statement of requirements and the Supplier will provide the Buyer with the Professional Services needed based on the Buyer's requirements.

Standard SMS Communications Service

Table 1 – SMS Communications Service provides access for SMS Users with access to basic reports. No Set Up Charge applies. Charges are per API.

[redacted]

Table 2 – UK Short Codes, UK Virtual Mobile Number, Keywords, and VPN

[redacted]

Table 3 – UK SMS message charges

SMS messages have a 160-character limit. Where multiple SMS are concatenated to accommodate longer messages, the Charges will apply to each SMS segment used.

[redacted]

Rich Communications Service (RCS) Business Messaging

RCS is a next generation SMS protocol that couples the ubiquity of SMS with the power of rich and contextual communications. The RCS Business Messaging module will allow the Buyer to create RCS messages using the drag and drop editor and send RCS messages to RCS-enabled devices and each module ordered will provide 75 Users.

[redacted]

Table 4 – RCS Module, API and Agent.

[redacted]

* Connect API will be provided without Charge when ordered as first API on Corporate Plan.

**RCS Agent – a conversational entity that users interact with. One agent is created for each brand the Buyer manages.

Table 5 – RCS Messages.

[redacted]

Conversational AI

Each Conversational AI solution requires a licence, a set-up, and an implementation package. All message channel costs are additional and as listed separately in this price card. In the case of the custom package, the setup fee and implementation package are combined into one charge.

Conversational AI Core: Includes 2 Channels, 1 Language, 2 integrations and up to 2000 requests per month as standard.

Conversational AI Plus: Includes 5 Channels, 3 Language, 5 integrations and up to 10,000 requests per month as standard.

Conversational AI Custom: Includes 5 Channels, 3 Language, 5 integrations and up to 30,000 requests per month as standard.

Table 6a – Conversational AI Licence Charges

[redacted]

Table 6b – Conversational AI Set-Up Charges

[redacted]

[redacted]

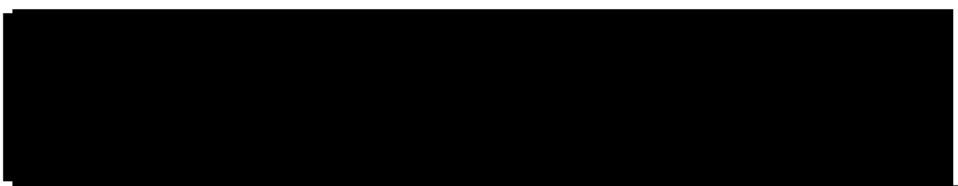
*Includes up to 15 set up and build days, additional days are charged at the custom day rate outlined in Table 8.

Table 6c – Conversational AI Implementation Package Charges

Table 7 - Conversational AI Additional Services

Table 8 – Professional Services

*Working Days only. Excludes travel and accommodation.



Advanced SMS and Multi-Channel Platform Connect Plans

The Supplier offers three enhanced Plans on top of the Standard SMS Communications Service, to support the Buyer's business with the right level of capability. The CONNECT Plans provide the Buyer the ability to tailor the Buyer's adoption, to optimise the Service and Charges to the Buyer's business needs.

The CONNECT Plans are designed for simple usage.

PLUS Plan - five licensed Users with additional support, SMS functionality and basic reports. Policy control includes user license allocation and hierarchy management and source address control. 8x5 email support with one Working Day response time.

PREMIUM Plan - 25 licensed Users with a multi-channel capability including SMS, email and voice, extra support and basic reports adding summary and export functionality on reports. Policy control includes user license allocation and hierarchy management and source address control and consent management. 24x5 email support with eight hours response time.

CORPORATE Plan - 75 licensed Users with full CPaaS (Communication Platform as a Service) capabilities including many other channels as RCS, other social media, and applications and modules that in the CORPORATE CPaaS plan can be bundled into vertical services) and a higher support level which allows usage of the Supplier's platform with all the most advanced options available in the market. Report functionality as above with the ability to schedule reports. Policy control includes user license allocation and hierarchy management and source address control and adding time zone, open hours, credit and cost centre controls. 24x7 email support with four hours response time on the CORPORATE Plan.

Charges are monthly unless otherwise indicated.

Table 9 – WebSMS Service.

[redacted]

Table 10 – WebSMS Short Codes. Charges are per code.

[redacted]

Table 11 – WebSMS APIs. Charges are per API integration.

[redacted]

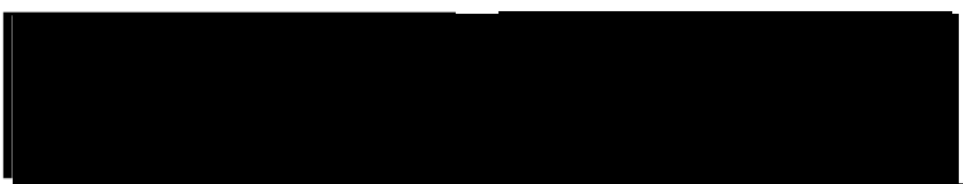
[redacted]

Table 12 – WebSMS modules. Charges are per plan.

Table 13 – Multi-channel Service.

Table 14 – Multi-channel Short Codes.

Table 15 – Multi-channel APIs. Charges are per API integration.



[redacted]

Table 16 – Multi-channel modules. Charges are per plan.

[redacted]

Table 17 – Multi-channel applications and features. Charges are per plan.

[redacted]

Table 18 – Corporate as a Service.

[redacted]

Table 19 – Corporate as a Service Short-Codes. Charges are per code.

[redacted]

Table 20 – Corporate as a Service APIs. Charges are per API integration.

Table 21 – Corporate as a Service module.

* Inbound Charge is per 10 keywords.

Table 22 – Corporate as a Service applications and features.

Table 23 Corporate as a Service Bundles. The CORPORATE Plan supports predefined and custom Corporate as a Service Bundles. These Bundles work on 75 Licences (valid for APIs, modules, applications, and additional features)

Order of Precedence

In the event of a conflict between the terms and conditions included within this Service Offer and the RM6116 Framework or Call-Off terms, then the Framework or Call-Off terms will take precedence.

Smart Messaging (Tailored Service) Annexes

Annex 1 - Joint Schedule 11 - Processing Data

This Annex is the standard data processing annex for the Service. The Supplier is happy to clarify any points with the Buyer prior to completion of an Order and entering into a Call-Off Contract.

Annex 1: a) Processing Personal Data – Contract Administration

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

- The contact details of the Relevant Authority's Data Protection Officer are to be provided by the Buyer:
- The contact details of the Supplier's Data Protection Officer are as follows:

  Name: Matthew Dalby
  Role: Director of Data Regulation and Compliance
  Email: ccsframeworks@bt.com

- The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- Any such further instructions shall be incorporated into this Annex.

Processing Personal Data – the Service

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Paragraph 3 to Paragraph 16 of Joint Schedule 11 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor.
Duration of the Processing	Duration of the Call-Off Contract plus 7 years post Call-Off Contract expiry.
Nature and purposes of the Processing	In respect of the Supplier Personal Data, CCS (and any other Relevant Authority) may: collect, collate, share, evaluate, use, store, replicate, and otherwise Process the Personal Data (subject to the terms of the Contract) to enable it to administer the Contract and fulfil tasks in the public interest and as required by law. This may include: • inviting the Supplier Staff to contract management workshops and events; • complying with requirements under the Contract to contact named individuals; • establishing the Supplier's compliance with the procurement process and the Contract; and • including Personal Data within reports. In respect of the Relevant Authority's Personal Data over which the Supplier shall act as a Processor, the Supplier may: collect, collate, share, evaluate, use, store, replicate, and otherwise Process the Personal Data (subject to the terms of the Contract) to enable it to administer and fulfil its obligations under the Contract. This may include: • complying with requirements under the Contract to contact named individuals; and • including Personal Data within reports.

[redacted]

Description	Details
	Service Related The Services provide the Buyer with a communications service. The Supplier processes any information that is generated by the User's use of voice mail, voice recording, text messaging features and web browsing. Given that recordings can be made and stored, any type of Personal Data could be captured or provided inadvertently by the User. Any access to the content of such communications by the Supplier is strictly in accordance with Law. The Supplier and its suppliers, including any Sub-processors of the Supplier and its suppliers, may from time to time use back-office support and system functions which are located or can be accessed by Users from outside of the UK and/or the European Economic Area. Any such processing will be in accordance with Joint Schedule 11 Paragraph 6 (d) (i) to (iv). The Buyer consents to the disclosure and transfer of Government Data, including Personal Data, as required in order to provide the Services. Due to the nature of the Services, Government Data will not be backed-up by the Supplier.
Type of Personal Data	• name; • gender; • date of birth; • email address; • address; • telephone number; • associated persons; • contact notes from calls; • contact records; • family and friends' telephone numbers; • Personal Data traffic and communications records; and This list is not exhaustive as the Buyer will specify what Buyer Personal Data is processed.
Categories of Data Subject	• Users • Third party participants in voice calls or text messages to and from Users
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data for a different duration	Duration of the Call-Off Contract plus 7 years post Call-Off Contract expiry

[redacted]

Annex 2 – Transparency Reports

Annex A of Call-Off Schedule 1 (Transparency Reports)

Please note the Supplier's Transparency Reports provide Buyers with a minimum reporting capability, which allows Buyers to directly manage their inventories for their services set out in their Call-Off Agreement.

Title	Content	Format	Frequency
Call-Off Charges	Details of usage and related costs will be provided on a monthly basis.	Emailed report and invoice	Monthly
Inventory	Users have access to a web portal, to view message usage volumes, by time and date.	User portal	User access 24/7/365

[redacted]

Annex 3 – Definitions

The following definitions shall apply, in the event of any conflict between Framework and Supplier definitions then the Framework definitions take precedence:

"**Administrator**" means any individual(s) authorised by the Buyer who is responsible for administering Users.

"**Alphanumeric Codes**" or "**Alpha Tags**" means any numeric or alphanumeric string used to send a Message in place of a standard international format phone number, and which complies with technical specifications issued by the Supplier or its suppliers from time to time.

"**API**" means any Application Programming Interface(s) provided to the Buyer to facilitate the Buyer's use of the Service.

"**Buyer Data**" means all data, including all text, sound, or image files and software provided to the Supplier or the Supplier's licensors (or both) by the Buyer or on the Buyer's behalf through the Buyer's use of the Service, and may include Personal Data.

"**Buyer Portal**" means https://tailored.bt.com/ or any other externally accessible website made available to the Buyer by the Supplier to provide for one or more specific functions in relation to the Service.

"**Communications Provider**" or "**CP**" means a person or company who provide an electronic communications network or an electronic communications service.

"**Content**" means information made available, displayed or transmitted in connection with the Service including applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

"**Critical Incident**" means a complete system failure leading to complete loss of system functionality or a loss of a major function or feature such as the failure to send, receive or process Messages.

"Customer Committed Date" means the date provided by the Supplier on which delivery of the Service (or each part of the Service, including to each Site) is due to commence.

"**EE**" means EE Limited, a wholly owned subsidiary of the Supplier Registered in England and Wales (company number 02382161) whose registered address is Trident Place, Mosquito Way, Hatfield, Hertfordshire, AL10 9BW, or as amended from time to time.

"**Eligible Contributory Spend**" means the Buyer's spend on UK Mobile SMS (excluding VAT) at the UK Mobile SMS Committed Price during each calendar month of the Minimum Period of Service, which contributes to achieving the Buyer's UK Mobile SMS Committed Spend and excludes the Buyer's spend on other types of SMS (including landline and international SMS), APIs, Short Codes, and any other Charges payable by the Buyer under the Call-Off Contract.

"**End Recipient**" means any individual, corporation or other legal entity to whom the Buyer or the Buyer's Users send or purport to send Messages using the Service.

"EULA" means an end user licence agreement for the COTS and non-COTS Software.

"Incident" means an unplanned interruption to, or a reduction in the quality of, the Service or particular element of the Service.

"Maintenance" means any work on the Supplier's network or Services, including to maintain, repair or improve the performance of the Supplier's network or Services.

"**Major Incident**" means garbled/corrupted Messages or Message content, general upgrade failures or failure of any application software.

[redacted]

"**Message Delivery**" means the transmission of any Message the Buyer or the Buyer's Users send from the Buyer Portal to the first Provider in the Provider Chain in a form and manner that allows that Provider to deliver the Message to the next Provider in the Provider Chain or to the End Recipient (as the case may be).

"**Minimum Period of Service**" means the period beginning on the Service Availability Date as set out in the Price Card. For the avoidance of doubt this does not affect the Buyer's right to terminate the Services during that period in accordance with Clause 10.2.2 of the Core Terms.

"**Mobile Network**" means the EE electronic communications network(s) from time to time operated by or on behalf of EE (and any part of such network(s)).

"**Network Operator**" means EE and any other mobile communications system network operator which provides wireless or mobile voice and data services to End Recipients.

"**One-Off Charges**" means those Charges set out in the Price Card in relation to the set up or connection of the Service (or any part thereof) or any Buyer Equipment or Supplier Equipment as applicable.

"**Professional Services**" means those services provided by the Supplier which are labour related services to assist with the implementation, configuration or management of the Service.

"**Provider**" means a Network Operator, Communications Provider or an aggregator whose services or infrastructure directly or indirectly receive a Message submitted by the Buyer to the Service for sending to the relevant End Recipient.

"**Provider Chain**" means the network of one or more Providers through which a Message may flow when the Buyer uses the Buyer Portal to transmit a Message before the Message is actually delivered to the End Recipient's handset.

"Purchased Equipment" means any equipment, including any Software, that the Supplier sells or licenses to the Buyer.

"Recurring Charges" means the Charges for the Service or applicable part of the Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Price Card.

"**Regulatory Body**" means any national or supranational regulatory or competition body, government department, court, or other body authorised and empowered under local law in the relevant country to regulate or adjudicate on the provision, receipt or use of the Service.

"**Rich Communications Service**" means the standards-based carrier messaging protocol which leverages data connectivity to deliver ubiquitous, next-generation messaging features.

"**Service Availability Date**" means the date (for each Service) on which that Service is first made available to the Buyer.

"**Service Desk**" means the helpdesk that the Buyer is able to contact to submit service requests, report Incidents and ask questions about the Service and which is available during Working Hours.

"**Service Management Boundary**" has the meaning given in Paragraph 1

"**Short Code**" means a set of digits, generally four to five digits long, used to enable End Recipients to send Messages to the Buyer or to access the Buyer's services (including any dedicated Short Code or shared Short Code).

"**SMS**" or "**Message**" means short message service comprising numerals, text or both of no more than 160 characters which conforms to the GSM character set for SMS or binary data which is base 64 encoded to a maximum length of 190 characters, or the permitted message format for the relevant Channel, sent by (or to) the Buyer or the Buyer's Users using the Service.

"Software" means Specially Written Software, COTS Software and non-COTS Supplier and third-party Software as described in the Contract that the Supplier provides to the Buyer as part of a Service. It includes any embedded software but excludes Open-Source Software.

[redacted]

"**Spend Measurement Date**" means the last day of each calendar month after the Service Availability Date or, where the Call-Off Contract or the Service is terminated within the Minimum Period of Service, the date on which the Call-Off Contract or the Service is terminated.

"**Ticket**" means the unique reference number provided by the Supplier for an Incident and that may also be known as a "fault reference number".

"**Total Eligible Contributory Spend**" means the Buyer's total Eligible Contributory Spend from the Service Availability Date.

"**UK Mobile SMS**" means SMS to be terminated on UK registered mobile number.

"**UK Mobile SMS Achieved Figure**" means the total number of UK Mobile SMS sent by the Buyer over any calendar month during the Minimum Period of Service.

"**UK Mobile SMS Commitment Option**" means, where the Buyer is eligible, the pricing option where the Buyer commits to a UK Mobile SMS Committed Volume in order to obtain the UK Mobile SMS Committed Price per UK Mobile SMS (if that option is selected by the Buyer in the Order Form).

"**UK Mobile SMS Committed Price**" means the discounted price per UK Mobile SMS sent (excluding VAT) during the Minimum Period of Service, as set out in the Order Form.

"**UK Mobile SMS Committed Spend**" means the level of spend (excluding VAT) to which the Buyer commits for UK Mobile SMS in each calendar month of the Minimum Period of Service, as set out in the Order Form.

"**UK Mobile SMS Committed Volume**" means the total number of UK Mobile SMS set out in the Order Form which the Buyer commits to send during each calendar month of the Minimum Period of Service.

"**Usage Charges**" means the Charges for the Service or applicable part of the Service that are calculated by multiplying the volume of units used or incurred by the Buyer or the Buyer's Users in a period (e.g. number of Messages sent using the Service, number of agents using the Service, or the number of minutes the Service was used for) with the relevant fee as set out in any applicable Price Card.

"User" means any person who is permitted by the Buyer to use or access a Service.

"**User Security Details**" means access profiles, IDs, usernames, personal identification numbers and passwords.

"WEEE" means waste electrical and electronic equipment.

"WEEE Directive" means the Waste Electrical and Electronic Equipment Directive 2012.

"Working Hours" means between the hours of 0800 and 1700 in a Working Day.

[redacted]

Annex 4 – Key Subcontractors

Soprano Design Ltd

[redacted]

1689 Smart Messaging Service Renewal for NHS Black Country ICB Order Form DRAFT (003)

Final Audit Report 2024-04-18

Created:	2024-04-12
By:	Smart Messaging (smenquiries@bt.com)
Status:	Signed
[redacted]	

"1689 Smart Messaging Service Renewal for NHS Black Countr y ICB Order Form DRAFT (003)" History

[redacted]