



**RM6100 Technology Services 3 Agreement
Framework Schedule 4 - Annex 1
Lots 2, 3 and 5 Order Form**

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 awarded on 16 June 2021 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website <https://www.crowncommercial.gov.uk/agreements/RM6100>. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed "Order Form";
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

- 1.1 the Framework, except Framework Schedule 18 (Tender);
- 1.2 the Order Form;



- 1.3 the Call Off Terms; and
- 1.4 Framework Schedule 18 (Tender).

Section A

General information

Contract Details	
Contract Reference:	WP2083
Contract Title:	Emergency Alerts Services
Contract Description:	<p>The Supplier will iterate and support the Emergency Alerts Service as it gets officially launched and used in a number of emergency scenarios. The Buyer will maintain overall accountability for the service. The Supplier will be responsible for all the technical delivery, design iterations and 24/7 operational support of the service. The Supplier will work as part of a blended Agile, multidisciplinary team with 2 permanent civil servants who will provide the strategic direction and will be responsible for the prioritisation decisions for the service. The blended team will report on delivery progress, risks and issues through established GDS governance processes.</p>
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	<p>The estimated Contract Value for Year 1 is £1,013,200 with a contingency to increase the value up to £1,600,000 (excluding VAT)</p> <p>Subject to further approval the Total Contract Value may be uplifted to £5,000,000.00 (excluding VAT).</p>
Estimated Year 1 Charges:	<p>up to £1,600,000.00 (excluding VAT) Maximum. Please refer to Attachment 2 - Charges and Invoicing.</p>
Commencement Date: this should be the date of the last signature on Section E of this Order Form	10 October 2022



Buyer details

Buyer organisation name

Cabinet Office: 1 Horse Guards Road, London, SW1A

Government Digital Service: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

Billing address

Invoices will be automatically sent to

[Redacted]

Buyer representative name

[Redacted]

Buyer representative contact details

Email:

[Redacted]

High Street, London, E1 8QS

Buyer Project Reference

WP2083 Emergency Alerts Services

Supplier details

Supplier name

Fujitsu Services Limited

Supplier address

Lovelace Road, Bracknell, RG12 8SN

Supplier representative name

Name:

[Redacted]

Supplier representative contact details

Email Address:

[Redacted]

Address: The Lantern, 75 Hampstead Road, London, NW1 2PL

Telephone:

[Redacted]

Order reference number or the Supplier's Catalogue Service Offer Reference Number

A unique number provided by the supplier at the time of the Further Competition Procedure. Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier's Catalogue Service Offer Reference Number.

945593



Guarantor details

Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.

Guarantor Company Name

The guarantor organisation name

Not Applicable

Guarantor Company Number

Guarantor's registered company number

Not Applicable

Guarantor Registered Address

Guarantor's registered address

Not Applicable



Section B

Part A – Framework Lot

Framework Lot under which this Order is being placed

Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.

- | | |
|--|-------------------------------------|
| 1. TECHNOLOGY STRATEGY & SERVICES DESIGN | <input checked="" type="checkbox"/> |
| 2. TRANSITION & TRANSFORMATION | <input type="checkbox"/> |
| 3. OPERATIONAL SERVICES | |
| a: End User Services | <input type="checkbox"/> |
| b: Operational Management | <input checked="" type="checkbox"/> |
| c: Technical Management | <input type="checkbox"/> |
| d: Application and Data Management | <input checked="" type="checkbox"/> |
| 5. SERVICE INTEGRATION AND MANAGEMENT | <input type="checkbox"/> |

Part B – The Services Requirement

Commencement Date

See above in Section A

Contract Period

Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	36 (3)
3	60 (5)
5	60 (5)

Initial Term Months

36 months to 09 October 2025

Extension Period (Optional) Months

1 period of up to 12 months - subject to Cabinet Office Approval.



With break review point clauses (in accordance with Clause 35.1.9 of the Call-Off Terms) at:

- 31 March 2023
- 09 October 2023
- 09 October 2024

Minimum Notice Period for exercise of Termination Without Cause 30 Calendar days
(Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)*

Sites for the provision of the Services

Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.

The Supplier shall provide the Services from the following Sites:

Buyer Premises:

Government Digital Service: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

Supplier Premises:

Lovelace Road, Bracknell, RG12 8SN

Third Party Premises:

Not Applicable

Buyer Assets

Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms

The Buyers Assets are:

- [REDACTED]

Additional Standards

Guidance Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.

The Buyer requires the Supplier to comply with the following additional Standards for



this Order Form:

- The Services must be delivered as per the GDS Service Manual (e.g. agile delivery aligned to scrum methodology) or other methodologies as agreed by the parties.
- The Supplier should follow where applicable to the Services:
 - The Government Technology Code of Practice (<https://www.gov.uk/government/publications/technology-code-of-practice>)
 - The Government Service Standard and Service Manual (<https://www.gov.uk/service-manual/service-standard>)
 - Resources to be supplied in accordance with DDAT Competency framework guidelines; <https://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework>
 - NCSC guidance <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>
 - The Government Digital Service Way (<https://gds-way.cloudapps.digital/>):
- Resources shall have the prescribed level of security clearance:
 - SC Clearance for all resources
 - All Supplier resources, including Sub-Contractors and partners, working on the project must be aware of and observe their obligations and responsibilities around confidentiality and protection of data as set out in the terms and conditions of this Order Form and applicable Schedules.
- GDS secure devices to be issued by the Buyer to the Supplier team undertaking the Services.



Buyer Security Policy

Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.

The **Supplier** will ensure compliance with;

GDS Secure Developer Information Assurance Schedules

<https://drive.google.com/file/d/1d9LV0RulfEHHiKByRFZQImW7P4CIRhok/view?usp=sharing>

Government Functional Security Standard No.7

<https://www.gov.uk/government/publications/government-functional-standard-govs-007-security>

The **Buyer and Supplier** will ensure compliance with;

The Government Cyber Security Strategy 2022 - 2030 and the Cyber Assessment Framework (CAF): <https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance>.

Minimum Cyber Security Standard (MCSS) to be met.

<https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>

The Cabinet Office Security requirements published here

<https://intranet.cabinetoffice.gov.uk/information-physical-and-personnel-security/> shall apply to the extent relevant to the provision of the Services. The Buyer will provide access to the Supplier to these requirements.

The Supplier shall ensure that the Supplier Personnel do not send unauthorised, accidental or malicious alerts.

Buyer ICT Policy

Guidance Note: where the Supplier is required to comply with the Buyer's ICT Policy then append to this Order Form below.

The Cabinet Office ICT Policy shall apply. The Supplier will have to agree to Cabinet Office ICT Policy to ensure when using The Buyers equipment and accepting 'Acceptable Use Policy'.

Insurance

Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.

Third Party Public Liability Insurance (£) - 1,000,000

Professional Indemnity Insurance (£) - 1,000,000



The insurance(s) required will be:

- a minimum insurance period of 6 years following the expiration or ending of this Contract
- Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the Technology Service 3. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit required by Law
- Employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
- Cyber and Data Protection Insurance

Buyer Responsibilities

Guidance Note: list any applicable Buyer Responsibilities below.

The Buyer shall have the following responsibilities:

- The Buyer will provide appropriate cloud hosting services and accounts to the Supplier to host the service
- The Buyer will provide access to the Notify and Emergency Alerts application as appropriate to allow the Supplier to fulfil its obligations in this Contract
- The Buyer will provide all the necessary licences, software, devices and technical infrastructure to ensure the Supplier can fulfil its obligations and deliver the service
- Procure the necessary services from and manage the Mobile Network Operators for the Emergency Alerts Service
- The Buyer will provide appropriate knowledge transfer to the Supplier prior to service handover
- The Buyer will provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Contract
- The Buyer will procure for the Supplier such agreed access and use of the Buyer Premises (as a licensee only) and facilities (including relevant IT systems) as is reasonably required for the Supplier to comply with its obligations under this Contract, such access to be provided during the Buyer's normal working hours on each Working Day or as otherwise agreed by the Buyer (such agreement not to be unreasonably withheld or delayed)
- The Buyer will agree a process and any changes required for other Government departments to raise incidents on the service
- The Buyer will provide the roles indicated (Product Manager and Technical Architect) for this service
- The Buyer will agree and provide the policy for using the service and confirm to the Supplier when new Government departments need to be onboarded
- The Buyer shall meet its obligations as set out in the Implementation Plan and shall do so on the dates identified in respect of such in the Implementation Plan.
- The Buyer will provide resources to audit accessibility standards of the service
- The Buyer will provide access to the respective GitHub accounts for the Service.
- The Buyer will provide approved for use laptops for those Supplier Personnel with privileged access to the system including the use of Yubikeys for security.

Goods



Guidance Note: list any Goods and their prices.

Not Applicable

Governance – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	<input checked="" type="checkbox"/>
Part B – Long Form Governance Schedule	<input type="checkbox"/>

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	<input checked="" type="checkbox"/>
Part B – Long Form Change Control Schedule	<input type="checkbox"/>

The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):

- for the purpose of Paragraph 3.1.2 (a), the figure shall be £[insert details]; and
- for the purpose of Paragraph 8.2.2, the figure shall be £[insert details].



Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses (see Annex 3 of Framework Schedule 4)

This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules

Guidance Note: Tick any applicable boxes below

Additional Schedules	Tick as applicable
S1: Implementation Plan	No
S2: Testing Procedures	No
S3: Security Requirements (either Part A or Part B)	Part A <input type="checkbox"/> or Part B <input checked="" type="checkbox"/>
S4: Staff Transfer	No
S5: Benchmarking	No
S6: Business Continuity and Disaster Recovery	<input checked="" type="checkbox"/>
S7: Continuous Improvement	No
S8: Guarantee	No
S9: MOD Terms	No

Part B – Additional Clauses

Guidance Note: Tick any applicable boxes below

Additional Clauses	Tick as applicable
C1: Relevant Convictions	No
C2: Security Measures	<input checked="" type="checkbox"/>
C3: Collaboration Agreement	No

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses

Guidance Note: Tick any applicable boxes below

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	No
Northern Ireland Law	No
Joint Controller Clauses	No

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.



Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)

Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.

- The Supplier shall provide a Security Management Plan under Paragraph 4.1 of Schedule S3 Part B shall be within 30 Working days of the Commencement Date.
- The Supplier to engage in any Buyer led Security Management Reviews of the Services (as part of contract management review)

Additional Schedule S4 (Staff Transfer)

Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.

Not Applicable

Additional Clause C1 (Relevant Convictions)

Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.

Not applicable

Additional Clause C3 (Collaboration Agreement)

Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.

Not Applicable

An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Commencement Date:

Not Applicable



Section D


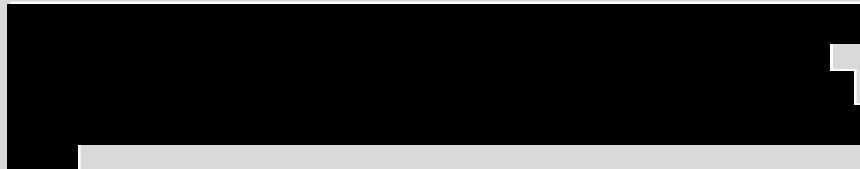



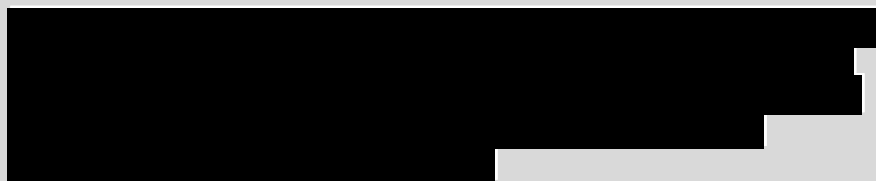
Supplier Response

Commercially Sensitive information

Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

Number	File Name	Date
1	[REDACTED]	[REDACTED]
1	[REDACTED]	[REDACTED]
1	[REDACTED]	[REDACTED]
1	[REDACTED]	
1	[REDACTED]	
1	[REDACTED]	
1	[REDACTED]	
1	[REDACTED]	
1	[REDACTED]	





Section E

Contract Award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

For and on behalf of the Supplier

Name	Fujitsu Services Limited
Job role/title	[REDACTED]
Signature	<i>Matthew Vole</i>
Date	6th October 2022

For and on behalf of the Buyer

Name	Cabinet Office
Job role/title	[REDACTED]
Signature	<i>Charlotte Manning</i>
Date	07/10/2022



Attachment 1 – Services Specification

The following is in scope for delivery by the Supplier in this context “service” means the Emergency Alerts Service:

1. Managing the service, including the technical infrastructure required to deliver the cell broadcasting system (Emergency Alerts, including the web based user interface, the public facing alerts pages at www.gov.uk/alerts and the network integration with the MNOs).
2. Operating the technical infrastructure to the levels of performance, security and availability agreed; and adhere to cyber security essentials with NCSC guidance implemented in a future solution.
3. Ensuring compliance to GDPR on design of systems for data processing and protection.
4. Providing 24 hours a day, 7 days a week, 365 days a year technical support for the system and channels for the COBR Unit, system users, and mobile network operators to raise issues, in line with the agreed response timeframes
5. Adding and removing users from the system as requested by the COBR Unit or the MNOs, following the agreed process
6. Undertaking additional work as necessary to ensure the system remains performant, secure, and highly available over time in accordance with the terms of this Contract and in line with the service requirements agreed with the Emergency Alerts Working Group
7. Designing, testing and implementing on-going improvements to the technical infrastructure and user interface to continue to meet user needs, such as: improving alerting and monitoring on the system, add the ability to retract a previously published alert to www.gov.uk/alerts, add banner publishing to www.gov.uk/alerts, ability to edit live and template messages at approval stage, ability to select all major cities at the municipal level, ability to apply time limits, ability to draw a circle or shape from a point, automatic failover of VPN connections to Mobile Network Operators. These should meet the Service Standards. The Supplier will provide a multi-disciplinary agile team to address the agreed on-going improvements which will be prioritised by the GDS Product Manager and Technical Architect.
8. Determining the best way to meet the agreed functional and non-functional requirements of the technical infrastructure of the cell broadcasting system; as well as demonstrating to the other relevant parties and the Buyer how changes and enhancements meet the agreed functional and non-functional requirements.
9. Overseeing content published about the Emergency Alerts on GOV.UK
10. Organising and supporting regular integration tests with the MNOs.
11. Organising, overseeing and supporting a yearly penetration test, in line with the GDS Information Assurance team requirements. The results of the penetration test should be reviewed with the Buyer.
12. Ensuring mitigation of any risks identified from the penetration test within the tolerance levels and timeframes agreed by the Buyer
13. Identifying risks, threats and vulnerabilities to the service and presenting to the Buyer for consideration
14. Ensuring compliance with Accessibility standards such as WCAG2.1AA.



15. Delivery of a Business Continuity and Disaster Recovery Plan (BCDR) within one month of contract signing.
16. Decoupling the sending interface and backend for sending alerts (which is currently done through GOV.UK Notify (www.notifications.service.gov.uk)); the deployment of www.gov.uk/alerts from the Notify teams deployment tool to an appropriate deployment tool; the deployment of the integrations with the Mobile Network Operators from the Notify teams deployment tool (Concourse) to an appropriate deployment tool; the monitoring and alerting of the emergency alerts service from the Notify teams monitoring and alerting stack.
17. Migrating any part of the service currently hosted on the GOV.UK PaaS to a different hosting solution as the GOV.UK PaaS is being retired in 18 months.
18. Ensuring all technical choices are inline with the [GDS Way](#) and that significant approaches or changes are documented, reviewed, and approved by GDS Architecture leadership.
19. Supporting the public launch of the system, and any yearly national test messages
20. Fixing accessibility issues in the sending journey that have already been found by an external accessibility audit, and continuing to ensure compliance with Accessibility standards
21. Performing regular software updates, installing security patches within a timescale appropriate to the severity so as not to leave the system vulnerable, and ensuring suitable alerting is in place to identify and mitigate potential supply chain or library vulnerabilities.
22. Working with COBR Unit and GDS Information Assurance to design a new scalable onboarding journey for emergency responders (which includes police forces, fire departments and more)
23. Providing ongoing 24/7 technical support for the product in line with SLAs and agreed escalation times (30 mins required response time for P1 and P2 incidents, next working day response for other requests and issues).
24. Testing and fixing integration issues with MNOs
25. Signing certificate signing requests provided by MNOs for yearly rotation of security certificates
26. Monitoring performance and reporting to stakeholders as necessary.
27. Implementing any necessary changes based on performance monitoring
28. Collaborate with the Mobile Network Operators as necessary to ensure the service remains available in accordance with the Service Levels. For avoidance of doubt, the Supplier is not responsible for the management of the Mobile Network Operators for the Emergency Alerts Service.



29. Support GDS engagement as required with the multiple stakeholders who are involved in the delivery of the service, ensuring we meet commitments as part of an agreed common roadmap.
30. Providing Yubikeys or similar Webauthn security keys for your staff who will administer the service
31. Taking part in practice drills led by COBR Unit for if an emergency alert is sent accidentally or maliciously (known as a 'rogue message').
32. Complete yearly penetration tests and address any recommendations to the agreed tolerance levels and timescales
33. Responding to any emergency alerts sent accidentally or maliciously by working with the other relevant departments and take any technical actions required, for example shutting down the integrations with the Mobile Network Operators until the incident has been resolved, revoking user accounts. Runbook plays already exist for this. The Supplier will work closely with the Buyer during this situation.
34. Documenting the code and how to support the service appropriately on an ongoing basis
35. [Publishing code and configuration in the open](#) under the Open Government Licence, and follow [good practices](#) when doing so. Work to the assumption that all code and history will be open in the future.

As per Buyer's requirements 'WP2083 RM6100-Further-competition- Emergency Alerts service', published on 21 July 2022.



Attachment 2 – Charges and Invoicing

The estimated Contract Value for Year 1 is £1,013,200 (excluding VAT) with a contingency to increase the value up to £1,600,000 (excluding VAT)

Subject to further approval the Total Contract Value may be uplifted to £5,000,000.00 (excluding VAT).

Contract Year 1 Service Charges - £1,013,200.00 (excluding



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Invoice details

The Supplier will issue valid electronic invoices monthly in arrears. The Buyer will pay the Supplier within thirty (30) days of receipt of a valid invoice.

Who and where to send invoices to

Invoices should be sent by email to:

[REDACTED]

Invoice information required

All invoices must include the WP number and Purchase Order Number.

The Buyer will issue a Purchase Order Number within 15 Working Days of the Commencement Date.

Each invoice shall be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges and total charge for the invoice period, in sufficient detail to enable the buyer to validate the invoice.

Invoice frequency

Invoice will be sent to the Buyer, Monthly in arrears

Part A – Milestone Payments and Delay Payments - NOT APPLICABLE



Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



Part D – Risk Register

Risk Number	Risk Name	Description of risk	Timing	Likelihood	Impact (£)	Impact (description)	Mitigation (description)	Cost of mitigation	Post-mitigation impact (£)	Owner
1										
2										
3										



Part E – Early Termination Fee(s) -
An amount equivalent to one (1) month’s Service Charge calculated at the date of the Buyer’s notice to terminate.



Attachment 3 – Outline Implementation Plan

Specific Milestone calendar end dates will be agreed between the Buyer and the Supplier in the first week after the Commencement Date.

In this table references to “GDS” shall mean the Buyer.

#	Milestone	Deliverables <i>(bulleted list showing all Deliverables (and associated tasks) required for each Milestone)</i>	Milestone Date
M1	Kick-off, knowledge handover and onboarding	<ul style="list-style-type: none">• Kick off meetings completed,• Ways of working confirmed• GDS and the Supplier define and agree any additional KPIs for Emergency Alerts that are not covered by Service Levels• Handover and initial knowledge transfer from GDS completed• Provide Yubikeys or similar Webauthn security keys for Supplier Personnel who will administer the service <p>Supplier to undertake discovery of the Buyer's existing system that the Supplier is to support and document as they see fit. Any issues the Supplier discovers, from what the Supplier has been able to identify from the access and information provided by the Buyer, that require rectification will be raised and the parties will agree an action plan for these to be remedied.</p>	Complete within 4 weeks from Commencement Date
M2	Business Continuity	<ul style="list-style-type: none">• Supplier team run high-level exercise to identify any significant issues which need to be tested and/or mitigated around potential disaster recovery scenarios. Team playback plan to GDS, Supplier and Buyer discuss and agree what needs to be mitigated before launch.	7 weeks from Commencement Date (or at least 2 weeks before the national welcome message whichever comes first)



		<ul style="list-style-type: none"> Supplier team create Business Continuity and Disaster Recovery Plan (BCDR) based on learnings, this is reviewed and approved by GDS including IA. Team have a plan to continually evolve and test the BCDR alongside platform changes, including incident management. 	<p>To complete within 5 months from the Commencement Date</p> <p>Ongoing</p>
M3	Public Launch of Emergency Alerts	<p>Support public launch of the Emergency Alerts System</p> <ul style="list-style-type: none"> This will include all necessary pre launch testing as reasonably stated by GDS There is also an expectation to support any yearly national test messages. 	By agreed launch date
M4	Decoupling with GOV.UK Notify	<ul style="list-style-type: none"> Decouple the sending interface and backend for sending alerts (which is currently done through GOV.UK Notify (www.notifications.service.gov.uk)). This will then involve hosting the sending interface and backend at a new location, likely www.emergencyalerts.service.gov.uk. Decouple the deployment of www.gov.uk/alerts from the Notify teams deployment tool (Concourse and an application running on PaaS to build the website) to an appropriate deployment Decouple the deployment of the integrations with the Mobile Network Operators from the Notify teams deployment tool (Concourse) to an appropriate deployment Decouple the monitoring and alerting of the emergency alerts service from the Notify teams monitoring and alerting stack Technical choices must be in line with GDS Way guidance and reviewed/approved by GDS Architecture leadership 	To complete within 5 months from Commencement Date



M5	Hosting	<ul style="list-style-type: none"> Move any part of the Emergency Alerts service currently hosted on the GOV.UK PaaS to a different hosting solution as the GOV.UK PaaS is being retired in 18 months Technical choices must be in line with GDS Way guidance and reviewed/approved by GDS Architecture leadership 	To complete 12 months from Commencement Date
M6	On-going improvements	<ul style="list-style-type: none"> Design, test and implement on-going improvements to the technical infrastructure and user interface to meet unmet user needs, such as: improving alerting and monitoring on the system, add the ability to retract a previously published alert to www.gov.uk/alerts, add banner publishing to www.gov.uk/alerts, ability to edit live and template messages at approval stage, ability to select all major cities at the municipal level, ability to apply time limits, ability to draw a circle or shape from a point, automatic failover of VPN connections to Mobile Network Operators; fixing issues with any existing functionality. <p>The Supplier will provide a multi-disciplinary agile team to address the agreed on-going improvements referred to above which will be prioritised by the GDS Product Manager and Technical Architect.</p>	To commence following completion of M1
M7	Accessibility	<ul style="list-style-type: none"> Maintain an Accessibility Statement for the Emergency Alerts service. Fix accessibility issues in the sending journey, and document any outstanding issues in the Accessibility Statement. Run a new external Digital Accessibility Centre accessibility audit (paid for by the Buyer) to confirm currently identified 	Ongoing following Commencement Date 6 months from Commencement Date 7 months from



		<p>accessibility issues have been resolved, and to identify new issues.</p> <ul style="list-style-type: none"> Fix any further accessibility issues that emerge from this audit 	<p>Commence ment Date</p> <p>within 3 months of second DAC audit</p>
M8	Support	<ul style="list-style-type: none"> Take over 24/7 live service support in line with agreed SLAs and agreed escalation times (30 mins required response time for P1 and P2 incidents, next working day response for other requests and issues). 	<p>4 weeks from Commence ment Date</p>
M9	Security	<ul style="list-style-type: none"> Ensure all Supplier personnel have read documentation on current known security risks and mitigations to the service which will be provided by GDS. Discuss any relevant points with GDS Information Assurance for further details if needed. Ensure all Supplier personnel observe their obligations to confidentiality and security and the risk associated with sending unauthorised accidental or malicious alerts. Complete yearly penetration test, report findings to GDS Information Assurance, address any agreed recommendations. The first penetration test will be completed as part of the decoupling of the service. Complete yearly threat modelling exercise, report findings to GDS Information Assurance, address any agreed recommendations. Suggest this one happens after the decoupling of the service is complete. 	<p>To be done within the first 2 months of the Commence ment Date</p> <p>From Commence ment Date</p> <p>Yearly</p> <p>Yearly</p> <p>Yearly</p>



		<ul style="list-style-type: none">• Sign certificate signing requests provided by Mobile Network Operators for yearly rotation of security certificates. This includes both VPN and TLS certificates. Up to 8 certificates in total per MNO per year.• Follow GDS runbook to manually rotate the CAP message signing key & certificate and provide new certificates to each of the MNOs. This will need to happen in the staging environment in December and the production environment in January.	By January 2023
M10	Reporting and documentation	<ul style="list-style-type: none">• Document the code, design decisions, research findings and how to support the service appropriately on an ongoing basis• Publish code in the open where appropriate• Reporting in line with 'Attachment 10'	Ongoing



Attachment 4 – Service Levels and Service Credits

Service Levels and Service Credits

All Service Levels will be measured across a Service Period of one month

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Accurate and timely billing of Buyer The Supplier to confirm with the Buyer accurate billing, before any invoice is raised	Accurate invoice with support information	accurate and on time at least 98% at all times	98%	Not applicable
24/7 live service support in line with agreed SLAs and agreed escalation times <ul style="list-style-type: none"> P1 (full outage or rogue messages) and P2 (substantial outage) incidents - 30 mins required response time Next working day response for other requests and issues For the avoidance of doubt, 'Response Time' is defined as Support acknowledging an alert or incident raised by the Buyer.	Availability Measured 24x7 over a Service Period other than during agreed maintenance windows.	at least 98% at all times	98%	Not applicable



Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
This Service Level will commence upon the completion of Milestone M8.				
<p>Uptime for the Emergency Alerts Service</p> <p>This Service Level will commence upon the completion of Milestone M8.</p>	<p>Availability</p> <p>Measured 24x7 over a Service Period other than during agreed maintenance windows.</p> <p>The service is considered to be down for the time that any of the following is true the ability to send alerts through the user interface is unavailable or severely degraded</p> <p>The ability to send alerts through the API is unavailable or severely degraded</p> <p>2 or more of the integrations with mobile network operators are unavailable or severely degraded</p>	At least 99.95%	99.95%	Not applicable



Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
	www.gov.uk/alerts is unavailable or severely degraded			

In measuring the Supplier's performance of the Services against the Service Levels, no account shall be taken of any measure in respect of any period of time or Incident or other measured event:

- (1) where the Supplier's failure to perform is as a result of the failure by the Buyer to meet any Buyer Responsibilities; or
- (2) where the Supplier has been prevented from or hindered in performing the Services by reason of an act or omission of the Buyer or of a third party other than one for whom the Supplier is contractually responsible; or
- (3) which arises as a consequence of a Force Majeure Event; or
- (4) where the Supplier and the Buyer have agreed that the Service Levels should be suspended or otherwise not operate; or

instances where through no fault of the Supplier to comply with its obligations under the Agreement access by the Supplier to Buyer Premises or Buyer or Buyer third party infrastructure required for the purposes of providing the Services either is not made available or is unreasonably delayed by the Buyer or Buyer third party.



Critical Service Level Failure

Critical Service failure is defined as:

- Failure to meet 24/7 live service support in line with the following Service Levels and agreed escalation times on 2 occasions in a rolling 60 day period.
 - P1 (full outage or rogue messages) and P2 (substantial outage) incidents - 30 mins required response time. (*Response time is measured between the time the incident is created in Pagerduty and the time it takes a responder to acknowledge the pagerduty alert, get to their computer and send a message in Slack or equivalent to say they are looking at it.*)
 - The Supplier does not need to update the Statuspage or fix the issue as part of the initial 30 mins response time.

P1 and P2 incidents are detailed in the [Emergency Alerts Support Runbook](#) (access will be given once onboarded).

- Supplier has failed to resolve 50% of the accessibility issues raised by the Buyer's current accessibility audit by 6 months from Commencement Date (as per Milestone 7). The resolution of the 50% of issues needs to be confirmed via a new audit from the Digital Accessibility Centre.
- Uptime falls below 99.95% (1 hour and 5 minutes) for a rolling 90 day period. The service is considered to be down for the time that any of the following is true
 - the ability to send alerts through the user interface is unavailable or severely degraded
 - the ability to send alerts through the API is unavailable or severely degraded
 - 2 or more of the integrations with mobile network operators are unavailable or severely degraded
 - www.gov.uk/alerts is unavailable or severely degraded

GDS will define severely degraded in detail with the supplier as part of the onboarding process.

Sending an 'Unauthorised Message'

- The supplier should not send any 'Unauthorised Message' from GOV.UK Notify or Emergency Alerts Services. The following constitute 'Unauthorised Message' is:
 - Any message (SMS, email, letter or emergency alert) that has not been expressly requested and authorised in writing by the Buyer (GDS) and/ or the COBR Unit. This includes both accidental or deliberate issuing of messages.

The Supplier fails to adequately protect the service resulting in:

Loss of personal data

Unauthorised third party accessing the system and Issuing a live message to the public.



The Supplier's responsibility for meeting the Service Levels shall be limited to the Supplier's environment only. For the avoidance of doubt, this shall exclude the infrastructures of third party telecommunications providers/MNO's, and the Amazon AWS platform. It also excludes third party provided services either managed by the Buyer or provided via the internet, for example but not limited to Notify.





Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

Part B – Key Sub-Contractors

Not Applicable



Attachment 6 – Software

- 1.1 The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).
- 1.2 The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

Part A – Supplier Software - not applicable

Part B – Third Party Software - not applicable



Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

PART A – CREDIT RATING THRESHOLD

Entity	Credit Rating (long term) <i>(insert credit rating issued for the entity at the Commencement Date)</i>	Credit Rating Threshold <i>(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3))</i>
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

Operational Board	
Buyer Members for the Operational Board	<div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>[Redacted]</div> <div>The personnel for Operation Board may change throughout the duration of the Order Form.</div>
Supplier Members for the Operational Board	<div>[Redacted]</div> <div>[Redacted]</div>



	<div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div>
Frequency of the Operational Board	Monthly
Location of the Operational Board	To be confirmed

PART B – LONG FORM GOVERNANCE - NOT USED

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, the following boards shall apply:



Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 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 Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED]

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED]

1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Buyer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none">• For the purposes of this contract, the Buyer is the Controller and the Supplier is the processor.• For the overarching Emergency Alerts service anticipated; GDS is the processor for DCMS and COBR Unit who will be Joint Controllers of the overarching service.• There is no personal data being relied on for this service as it relies on geo-location mast notifications for citizens in a given location where the alerts are targeted. <p>Emergency alerts work like a radio broadcast.</p> <p>In an emergency, mobile phone masts in the surrounding area will broadcast an alert. Every compatible mobile phone or tablet in range of a mast will receive the alert as a broadcast message.</p>
Duration of the processing	Contract Period



Nature and purposes of the processing	<p>The personal data is limited to Administrative access for those controlling and administering the service only.</p> <p>Note: Disclosure by transmission geo-location broadcast within specific locations where a potential severe or critical alert messaging is required to be broadcast to the citizen.</p> <p>Emergency alerts work on all 4G and 5G phone networks in the UK.</p> <p>There is no collection or sharing of data from citizen devices, nor collection of location when an alert is received.</p>
Type of Personal Data	<p>The personal data is limited to Administrative access for those control and administering the service only. This relates to; name and email address of the administrators. There is no personal data being captured for the citizens who will receive Emergency alerts, as this remains the responsibility of the mobile contract providers contractual relationship for their contracts and cannot be accessed or processed by the Emergence Alert teams.</p> <p>Administration data may also include correspondence such as complaints or queries as to the service.</p>
Categories of Data Subject	<p><i>Administrative staff</i></p>
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	<p>Supplier to destroy all copies of the Buyer Data when they receive Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law.</p>



Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
SLAs and KPIs	These will include 99.95% uptime for the service and 30 minute response time for P1 (full outage or rogue messages) and P2 (substantial outage) incidents.	Google slides or agreed dashboard	Monthly
Emergency Alerts team check-in	Delivery progress, risks, assumptions, issues, dependencies and overall assurance	Blended Emergency Alerts presents to GDS Digital Service Platforms senior management team Google slides	Fortnightly
Performance, contract and delivery management review	Run through team and individual performance against agreed delivery milestones and roadmap. Any issues with the quality and pace of delivery are flagged and clear next steps are agreed. Any individual performance issues are flagged and clear next steps are agreed. The Supplier must replace someone who is not suitable with a suitably qualified alternative within 20 working days	Google slides and meeting between GDS and supplier. This should include	Monthly



	Decisions are made about any changes in the people or skills needed - add or remove people		
Architecture review	Key technical, architectural, and security considerations	TBC	Quarterly and when needed
Regular show and tells	This will be presenting at different GDS events, such as the Digital Service Platforms monthly showcase, GDS show the thing	Google slides and meeting across Digital Service Platforms or GDS	Monthly
Charges	Invoice	PDF	On a monthly basis



Crown
Commercial
Service

Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses



1. Exit plan

- 1.1. The Supplier must provide an exit plan which ensures continuity of service and the Supplier will follow it.
- 1.2. When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 1.3. If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.
- 1.4. The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 1.5. Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 1.6. The Supplier acknowledges that the Buyer's right to extend the Term of this contract is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
 - 1.6.1. The Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
 - 1.6.2. there will be no adverse impact on service continuity
 - 1.6.3. there is no vendor lock-in to the Supplier's Service at exit
 - 1.6.4. It enables the Buyer to meet its obligations under the Technology Code Of Practice
2. If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
3. The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
 - 3.1. the transfer to the Buyer of any technical and design information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
 - 3.2. the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
 - 3.3. the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier



- 3.4. the testing and assurance strategy for exported Buyer Data
- 3.5. if relevant, TUPE-related activity to comply with the TUPE regulations
- 3.6. any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition



Annex 2 - Cabinet Office Travel and Subsistence Policy

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

Supplier organisations must also comply with the following:

1) Travel rates

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

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

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

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

Rail Travel

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

Air Travel

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

Taxis

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

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

All taxi fares should be receipted.

Hire a self-drive car

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

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



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

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

Personal Mileage Allowance

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

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

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

2) Subsistence rates

UK Lodging rate for rented accommodation

Ceiling - £37 per night.

UK Hotel accommodation rate

Ceiling for bed and breakfast:

London (from centre out to the M25 motorway ring road) - £130.00

Major cities (Aberdeen, Birmingham, Belfast, Bristol, Cardiff, Coventry, Edinburgh, Glasgow, Harlow, Leeds, Liverpool, Manchester, Middlesbrough, Newcastle, Oxford, Portsmouth, Reading, Sheffield, York) - £90.00

Elsewhere - All other locations not mentioned above - £85.

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

UK Meal allowance

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

one meal if away for over 5 hours

two meals if away for 10 to 12 hours

three meals if away for over 12 hours

The ceilings within which you may claim are:

£5 - breakfast

£5 - lunch



£18 - dinner

£23 - combined lunch and dinner

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

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

UK Personal Incidental Hotel Expenses - £5 per night

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

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

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

Overseas rates

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

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

Overseas staying with relatives or friends rate

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

Overseas personal incidental hotel expenses

days 1 to 4 = £5 per day

day 5 onwards = £10 per day

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