CONDITION DATA COLLECTION IT SOLUTION

CONTRACT

G-CLOUD SERVICES CALL-OFF TERMS

DEPARTMENT for EDUCATION

- and -

Kykloud Ltd

relating to

the provision of G-Cloud Services

Contents

Schedule 2: Call-Off Terms

Date	19th August 2016	**Order Reference**	EFA CDC IT SYSTEM

FROM:

Customer	The Secretary of State for Education **"Customer"**
Customer's Address	Sanctuary Buildings, Great Smith Street, London, SW1P3BT
Invoice Address	For paper invoices Central Payments Team 53-55 Butts Road, Coventry, CV1 3BHI FY5 3TA See additional guidance on submitting invoices at Section 6.2
Principal Contact	Name: Redacted Address: Redacted Phone: Redacted

TO:

Supplier	Kykloud Ltd **"Supplier"** SERVICE ID 6251588452614140
Supplier's Address	**Nautilus House, Redburn Court, Earl Grey Way, North Shields NE29 6AR**
Account Manager	Name: Redacted Address: Redacted Phone: Redacted

1.	**TERM**

1.1 Commencement Date

This Call-Off Agreement commences on: [19/08/2016]

1.2 Expiry Date

1.2.1 This Call-Off Agreement shall expire on: [18/08/2018]; or

1.2.2 the second (2) anniversary of the Commencement Date; whichever is the earlier, unless terminated earlier pursuant to Clause CO-9 of the Call-Off Agreement.

1.3 Services Requirements

1.3.1 This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services utilized by Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.

1.3.2 G-Cloud Services

1.3.2.1 Lot1 IaaS	N/A;
1.3.2.2 Lot 2 PaaS	N/A
1.3.2.3 Lot 3 SaaS	Service ID 6251588452614140

PDF
Kykloud Service Definition

1.3.2.4 Lot 4 Specialist G-Cloud Services	N/A

1.3.2.5 G-Cloud Additional Services
N/A

2. PRINCIPAL LOCATIONS

2.1 Principal locations where the services are being performed:

Kykloud Premises : Nautilus House, Redburn Court, Earl Grey Way, North Shields NE29 6AR

3. STANDARDS

3.1 Quality Standards

All delivered services will be in line with the quality standards offered or defined in the Gcloud service descriptions. In addition Kykloud will implement all of the responses given to questions for all sections of the Statement of Requirements, in particular responses for standards outlined in sections NRF014 and NRF015.

The development of requirements shall also:-

- adhere to the **DfE Architecture principles,** the general rules and guidelines that inform and supports the way in which DfE sets about fulfilling its mission;
- meet **Strategic characteristics**, or **Quality goals**, including reliability, portability, scalability etc, which will be used to judge the operation of the System;
- comply with **Government guidance** and **Policies**;
- **be secure** and include risk management and the DSAM process and
- **comply to standards**, such as ISO27001 and similar.

3.2 Technical Standards

All delivered services will be in line with the technical standards offered or defined in the Gcloud service descriptions. In addition Kykloud will implement all of the responses given to questions for all sections of the Statement of Requirements, in particular responses for standards outlined in sections NRF001 to NRF018 and SM001 to SM005.

The development of the requirements shall also:

- support the **DfE technical strategies**, which define the strategic vision to guide delivery of the DfE IT and Business modernisation programmes.

4. ONBOARDING

4.1 On-boarding

The requirements below need to be developed within 10 weeks of the contract being signed. There will be check points and agreed sign off points between the EFA – the Customer and Kykloud – the Supplier on the implementation and development phase. The implementation plan is detailed in schedule 8.. The dates for these will be agreed in writing between these two parties by no later than 19th August 2016.

There will also be an extensive period of User Acceptance Testing (UAT) once the implementation work has been completed as identtified in the Implementation programme.

The On-boarding of the IT Solution will be implemented in accordance with the whole of the Statement of Requirements issued to Kykloud on the 10th June with the response submitted on 7th July 2016. The Statement of Requirements and Kykloud's response are attached below . There was the additional clarification from the EFA and Kykloud response dated the 5th August 2016. This is attached below.

CDC IT Solution - Statement of Requirer

DFE EFA CDC Tender Response from Kyklou

EFA CDC Final Clarifications submitte

All of the requirements in each of the sections will need to be developed and implemented by Kykloud on their IT System and will cover the following:

Functional Requirements:	
FR001	Data Entry
FR002	Data Validation
FR003	Data Storage
FR004	Data Sourcing and live connectivity
FR005	Access
FR006	Viewing Data
FR007	Reporting
FR008	Commenting and Flagging
FR009	Help Support and Training
FR010	Assigning and Notifications
Non-Functional Requirements:	
NFR001	Integrity
NFR002	Recoverability
NFR003	Portabliity
NFR004	Performance
NFR005	Capacity
NFR006	Scalability
NFR007	Resilience
NRF008	System Availabilty
NFR009	Interoperabilty
NFR010	Modifiabilty

NFR011	Audit	
NFR012	Data Retention and Migration	
NFR013	Accessibilty	
NFR014	Data Standards	
NRF015	Open Standards	
NFR016	Security	
NFR017	Authenticiation	
NFR018	On-boarding and service implementation	
Service Management Requirements:		
SM001	Incident & Problem Management	
SM002	Operational Monitoring and alerting	
SM003	Service Reporting	
SM004	Change and Release Management	
SM005	Back-up and Archive Management	

5. CUSTOMER RESPONSIBILITIES

5.1 Customer's Responsibilities

The contract focus is on the delivery and implementation of all of the requirements FR001 to FR010, NRF001 to NRF018 and SM001 to SM005. The Customer responsibilities are outlined in section NFR018 of the Statement of requirements. In addition the Customer will make available the necessary resource needed for the implementation for all of the stated requirements and in accordance with agreed implementation plan, between the EFA and Kykloud.

5.1.1 The Customer Team

The implementation of the CDC IT System will consist of the following people from the Customer side

IT Project Manager

Leading Building Surveyor

Building Surveyor

CDC Programme Manager

IT Group

5.1.2 Service Management Meetings

There will be monthly service management meetings which both the Customer and Supplier need to attend. These meetings will be attended by the Service/Contract Manager who will ensure that all relevant reporting is completed in preparation for these meetings.

The Supplier Service Manager will report on the KPIs and Milestones for the monthly meetings call and they will be the contract escalation point and have overall responsibility for the Contract.

5.2 Customer's equipment

It is not anticipated that the Supplier will use any DfE equipment.

5.3 Raising Work Orders for Ad-Hoc Development

5.3.1 This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services utilized by the Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.

5.3.2 The Customer shall have the ability to raise work packages within the scope of the services covered by this agreement. Individual work packages will be agreed as and when required during the Agreement Period. All new requests for work within scope of the agreement shall be initiated by an authorized employee of the Customer by means of a 'Request for Quote' (RFQ) and emailed to the Supplier's nominated representative. Activities, outcomes and delivery milestones will be agreed as part of the Request for Quote process. The Process for the RFQ is outlined below.

EFA CDC Project Change Control v1 1(

The payment profile for each work package will be linked to milestones and outputs agreed between the Customer and Supplier before work initiation.

6. PAYMENT

6.1 Payment profile and method of payment

Charges payable by the Customer (including any applicable discount but excluding VAT), payment profile and method of payment (e.g. Government Procurement Card (GPC) or BACS)

Indicate preferred payment profile by selecting one from:

6.1.1 Monthly in arrears

The value of the contract is in accordance with Kykloud's response to the clarification issued. The total contract value amount for the 24th month period is [redacted] This is broken down as outlined in the pricing model and estimated pricing model below. This also includes the agreed rate card (fig 1 below) for any ad-hoc development work that is agreed between the EFA and Kykloud as set out in Non-Functional Requirement NRF018.

This is a fixed price contract and the payment schedule attached will be affective for the 2 years. This fixed price is based on there being no data storage limits set over the agreement period.

Any adhoc development work agreed will be in addition to the fixed price.

FIG 1 – Kykloud SFIA Rate Card

Appropriate SFIA Definition	SFIA Day Rate
[redacted]	[redacted]

6.2 Invoice format

The Supplier shall issue paper invoices, in arrears, on satisfactory completion of agreed work packages. The Customer shall pay the Supplier within thirty (30) calendar days of receipt of a

valid invoice, submitted in accordance with this paragraph 6.2, the payment profile set out in paragraph 6.1 above and the provisions of this Call-Off Agreement.

A valid invoice is one that is:

- Delivered in timing in accordance of the contract
- Is for the correct sum
- Is correct in terms of services/goods supplied
- Has a unique invoice number
- Quotes a valid Purchase Order number
- Includes correct Supplier details, date, contact details
- Invoicing will be in £ Sterling and payment will be made by BACS transfer.

Invoicing will be in £ Sterling

All queries regarding payments or the settlement of invoices shall be directed to the Customers Principle Contact : Anthony Campbell-Butler.

7. DISPUTE RESOLUTION

7.1 Level of Representative to whom disputes should be escalated to:

For DfE : Redacted– Head of Condition Data and Cost, Strategy and Intelligence Directorate

For Kykloud: Redacted

7.2 Mediation Provider

Centre for Effective Dispute Resolution.

8. LIABILITY

Subject to the provisions of Clause CO 11 'Liability' of the Call–Off Agreement:

8.1 The annual aggregate liability of either Party for all defaults resulting in direct loss of or damage to the property of the other Party (including technical infrastructure, assets, equipment or IPR but excluding any loss or damage to the Customer Data or Customer Personal Data) under or in connection with this Call–Off Agreement shall in no event exceed £1 million.

8.2 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off

Agreement shall in no event exceed £1 million of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period.

8.3 The annual aggregate liability under this Call–Off Agreement of either Party for all defaults shall in no event exceed the greater of £100,000 or one hundred and twenty five per cent (125%) per cent of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period.

9. INSURANCE

9.1 Minimum Insurance Period

Six (6) Years following the expiration or earlier termination of this Call-Off Agreement

9.2 To comply with its obligations under this Call-Off Agreement and as a minimum, where requested by the Customer in writing the Supplier shall ensure that:

- **professional indemnity insurance** is held by the Supplier and by any agent, Sub-Contractor or consultant involved in the supply of the G-Cloud Services and that such professional indemnity insurance has a minimum limit of indemnity of one million pounds sterling (£1,000,000) for each individual claim or such higher limit as the Customer may reasonably require (and as required by Law) from time to time;
- **employers' liability insurance** with a minimum limit of five million pounds sterling (£5,000,000) or such higher minimum limit as required by Law from time to time.

10. TERMINATION

10.1 Undisputed Sums Time Period

At least ninety (90) Working Days of the date of the written notice specified in Clause CO-9.4 of the Call-Off Agreement.

10.2 Termination Without Cause

At least thirty (30) Working Days in accordance with Clause CO-9.2 of the Call-Off Agreement.

11. AUDIT AND ACCESS

Twelve (12) Months after the expiry of the Call-Off Agreement Period or following termination of this Call-Off Agreement.

12. PERFORMANCE OF THE SERVICES AND DELIVERABLES

12.1 Implementation Plan and Milestones (including dates for completion)

The base line of the Implementation plan is in Schedule 8.

12.1.1 If so required by the Customer, the Supplier shall produce within one (1) Month of the Commencement Date a further version of the Implementation Plan (based on the above plan) in such further detail as the Customer may reasonably require. The Supplier shall ensure that each version of the Implementation Plan is subject to Customer's written approval. The Supplier shall ensure that the Implementation Plan is maintained and updated on a regular basis as may be necessary to reflect the then current state of the implementation transition and/or transformation of the G-Cloud Services.

12.1.2 The Customer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

12.1.3 The Supplier shall perform its obligations so as to achieve each milestone by the milestone date.

12.1.4 Changes to the milestones shall only be made in accordance with the Variation procedure as set out in Clause CO-21 and provided that the Supplier shall not attempt to postpone any of the milestones using the Variation procedure or otherwise (except in the event of a Customer default which affects the Supplier's ability to achieve a milestone by the relevant milestone date).

12.2 Service Levels

The Service levels will be in accordance with the requirements and response set out in SM001 to SM005 from the Statement of Requirements

The agreed Service levels between the Customer and Supplier are in the attachement below.

Contract 12 2 Service Level Additional Refer

13. COLLABORATION AGREEMENT

In accordance with Clause CO-20 of this Call-off Agreement, the Customer does not require the Supplier to enter into a Collaboration Agreement. However the Customer requires Supplier adherence to CO-20

DfE: Special Conditions for Contracts

DfE Library of Clauses

(NB : the numbering system reflects the number used on the full DfE library of clauses)

1. Intellectual Property Rights and Copyright

"Intellectual Property Rights"	means patents, trade marks, service marks, design rights (whether registerable or otherwise), applications for any of the foregoing, know-how, rights protecting databases, trade or business names and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom).
"the Act"	means the Copyright Designs and Patents Act 1988;
"Copyright"	means any and all copyright, design right (as defined by the Act) and all other rights of a like nature which may, during the course of this Contract, come into existence in or in relation to any Work (or any part thereof);
"Crown and/or Her Majesty"	both mean Queen Elizabeth II and any successor to Her Majesty;
"HMSO"	means Her Majesty's Stationery Office;
"Her Majesty's Government"	means the duly elected Government for the time being during the reign of Her Majesty and/or any department, committee, office, servant or officer of such Government;
"Work"	means any and all Works including but not limited to literary, dramatic, musical or artistic works, sound recordings, films, broadcasts or cable programmes, typographical arrangements and designs (as the same are defined in the Act) which are created from time to time during the course of this Contract by the Supplier or by or together with others at the Supplier's request or on its behalf and where such works directly relate to or are created in respect of the performance of this Contract or any part of it.

Copyright Warranties

1.3 The Supplier now warrants to the Crown, HMSO and the Department (and to any assignees and licensees of each) that all Works will not infringe in whole or in part any copyright or like right or any other intellectual property right of any other person (wheresoever) and agrees to indemnify and hold harmless Her Majesty and/or Her Majesty's Government against any and all claims, demands, proceedings, expenses and losses, including any of a consequential nature, arising directly or indirectly out of any act of the foregoing in relation to any Work, where such act is or is alleged to be an infringement of a third party's copyright or like right or other intellectual property right (wheresoever).

1.4 The warranty and indemnity contained in Clause 1.3 above shall survive the termination of this Contract and shall exist for the life of the Copyright.

2. Ownership of Drawings Specifications and Other Data

Any drawings, specifications or other data, as set out in Schedule x, completed or provided in connection with this Contract shall become or, as the case may be, remain the property of the Department and be delivered up to the Department at the times shown in Schedule x or on completion or termination of the Contract.

3. Not Used

4. Suppliers Standards –

The Supplier shall as far as practicable satisfy the Department that it operates to an acceptable standard such as BS 5750, BS EN ISO 9000 or an equivalent.

5. Issued Property – N/A

6. Suppliers Employees and Sub-Contractors

6.1 The Supplier shall give to the Department if so requested a list of all persons who are or may be at any time directly concerned with the performance of this Contract specifying the capacity in which they are concerned with the provision of the Services and giving such other particulars as the Department may reasonably require.

6.2 If the Department notifies the Supplier that it considers that an employee or sub-contractor is not appropriately qualified or trained to provide the Services or otherwise is not providing the Services in accordance with this Contract, then the Supplier shall, as soon as is reasonably practicable, take all such steps as the Department considers necessary to remedy the situation or, if so required by the Department, shall remove the said employee or sub-contractor from providing the Services and shall provide a suitable replacement (at no cost to the Department).

6.3 The Supplier shall take all reasonable steps to avoid changes of employees or sub-contractors assigned to and accepted to provide the Services under the Contract except whenever changes are unavoidable or of a temporary nature. The Supplier shall give at least one month's written notice to the Contract Manager of proposals to change key employees or sub-contractors.

7. Hazardous Materials – N/A

8. Steering Committee – N/A

9. Use of Premises

9.1 Unless otherwise agreed, any land or premises made available to the Supplier by the Department in connection with the provision of the Services shall be made available to the Supplier free of charge and without exclusive possession and shall be used by the Supplier solely for the purpose of providing the Services. The Supplier shall have the use of such land or premises as licensee and shall vacate the same on the expiry or other termination of this Contract.

9.2 The Supplier shall ensure that in providing the Services its employees and sub-contractors co-operate as far as may be reasonably necessary with the Department's employees. The Supplier shall further ensure that its employees and sub-contractors carry out their duties and behave while on the Department's premises in such a way as to cause no unreasonable or unnecessary disruption to the routine and procedures of the Department, its employees, visitor or other Suppliers.

9.3 The Supplier shall ensure that its employees and sub-contractors comply with all rules and regulations from time to time issued by the Department relating to the use and/or security of the Department's premises.

10. Facilities Provided

For the purpose of the Contract the following areas and facilities at the Department's premises will be provided free for use by the Supplier and its employees and sub-contractor:

Toilets
Cooking Facilities
Heating
Lighting
First Aid

The Supplier shall be responsible for ensuring that proper use and reasonable care is taken by it's employees and sub-contractors of facilities provided.

11. Data Protection Act

"Affiliate"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Supplier Personnel"	all employees, agents, Contractors and contractors of the Supplier and/or of any Sub-contractor;
"Control"	means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and **"Controls"** and **"Controlled"** shall be interpreted accordingly;
"Regulatory Bodies"	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Department and **"Regulatory Body"** shall be construed accordingly.
"Sub-contractor"	the third party with whom the Contractor enters into a Sub-contract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents;
"Working Day"	any day other than a Saturday, Sunday or public holiday in England and Wales.

11.1 With respect to the parties' rights and obligations under this Contract, the parties agree that the Department is the Data Controller and that the Supplier is the Data Processor. For the purposes of this Clause 11, the terms "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Process" and "Processing shall have the meaning prescribed under the DPA.

11.2 The Supplier shall:

11.2.1 Process the Personal Data only in accordance with instructions from the Department (which may be specific instructions or instructions of a general nature as set out in this Contract or as otherwise notified by the Department to the Supplier during the period of the Contract);

11.2.2 Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by law or any Regulatory Body;

11.2.3 Implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or

damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

11.2.4 Take reasonable steps to ensure the reliability of any Supplier Personnel who have access to the Personal Data;

11.2.5 Obtain prior written consent from the Department in order to transfer the Personal Data to any Sub-contractors or Affiliates for the provision of the Services;

11.2.6 Ensure that all Supplier Personnel required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Clause11;

11.2.7 Ensure that none of Supplier Personnel publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Department;

11.2.8 Notify the Department within five Working Days if it receives:

11.2.8.1 a request from a Data Subject to have access to that person's Personal Data; or

11.2.8.2 a complaint or request relating to the Department's obligations under the Data Protection Legislation;

11.2.9 Provide the Department with full cooperation and assistance in relation to any complaint or request made, including by:

11.2.9.1 providing the Department with full details of the complaint or request;

11.2.9.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Department's instructions;

11.2.9.3 providing the Department with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Department); and

11.2.9.4 providing the Department with any information requested by the Department;

11.2.10 Permit the Department or the Department's Representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Supplier's data processing activities (and/or those of its agents, subsidiaries and Sub-contractors) and comply with all reasonable requests or directions by the Department to enable the Department to verify and/or procure that the Supplier is in full compliance with its obligations under this Contract;

11.2.11 Provide a written description of the technical and organisational methods employed by the Supplier for processing Personal Data (within the timescales required by the Department); and

11.2.12 Not Process or otherwise transfer any Personal Data outside the European Economic Area. If, after the Commencement Date, the Supplier (or any Sub-contractor) wishes to Process and/or transfer any Personal Data outside the European Economic Area, the following provisions shall apply:

11.2.12.1 the Supplier shall submit a request for change to the Department which shall be dealt with in accordance with any Change Control Procedure

11.2.12.2 the Supplier shall set out in its request for change details of the following:

(a) the Personal Data which will be Processed and/or transferred outside the European Economic Area;

(b) the country or countries in which the Personal Data will be Processed and/or to which the Personal Data will be transferred outside the European Economic Area;

(c) any Sub-contractors or other third parties who will be Processing and/or transferring Personal Data outside the European Economic Area; and

(d) how the Supplier will ensure an adequate level of protection and adequate safeguards (in accordance with the Data Protection Legislation and in particular so as to ensure the Department's compliance with the Data Protection Legislation) in respect of the Personal Data that will be Processed and/or transferred outside the European Economic Area;

11.2.12.3 in providing and evaluating the request for change, the parties shall ensure that they have regard to and comply with then-current Department, Government and Information Commissioner Office policies, procedures, guidance and codes of practice on, and any approvals processes in connection with, the Processing and/or transfers of Personal Data outside the European Economic Area and/or overseas generally; and

11.2.12.4 the Supplier shall comply with such other instructions and shall carry out such other actions as the Department may notify in writing, including:

(a) incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) in this Contract or a separate data processing agreement between the parties; and

(b) procuring that any Sub-contractor or other third party who will be Processing and/or transferring the Personal Data outside the European Economic Area enters into a direct data processing agreement with the Authority on such terms as may be required by the Department, which the Supplier acknowledges may include the incorporation of standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation)."

11.3 The Supplier shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Department to breach any of its applicable obligations under the Data Protection Legislation.

12. Departmental Security Standards for ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	a level of security clearance described as pre-employment checks in the National Vetting Policy.
"CESG"	is the UK government's National Technical Authority for Information Assurance. The website is http://www.cesg.gov.uk/Pages/homepage.aspx
"CESG IAP" "CESG Information Assurance Policy Portfolio"	means the CESG Information Assurance policy Portfolio containing HMG policy and guidance on the application of 'security assurance' for HMG systems.
"CTAS" "CESG Tailored Assurance"	is an 'information assurance scheme' which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public

	sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks.
"CPA" "CESG Product Assurance"	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry.
"CCSC" "CESG Certified Cyber Security Consultancy"	is CESG's approach to assessing the services provided by consultancies and confirming that they meet CESG's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors.
"CCP" "CESG Certified Professional"	is a CESG scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors.
"CC" "Common Criteria"	the Common Criteria scheme provides assurance that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria.
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.
"Data" "Data Controller" "Data Processor" "Personal Data" "Sensitive Personal Data" "Data Subject", "Process" and "Processing"	shall have the meanings given to those terms by the Data Protection Act 1998
"Department's Data" "Department's Information"	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:

	(i) supplied to the Supplier by or on behalf of the Department; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
"DfE" "Department"	means the Department for Education
"Departmental Security Standards"	means the Department's security policy or any standards, procedures, process or specification for security that the Supplier is required to deliver.
"Digital Marketplace / GCloud"	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.
"FIPS 140-2"	this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled 'Security Requirements for Cryptographic Modules'. This document is the de facto security standard used for the accreditation of cryptographic modules.
"Good Industry Practice" "Industry Good Practice"	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"Good Industry Standard" "Industry Good Standard"	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"GSC" "GSCP"	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	means Her Majesty's Government
"SPF" "HMG Security Policy Framework"	This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.
"ICT"	means Information and communications technology (ICT) is used as an extended synonym for information technology (IT), used to describe the

	bringing together of enabling technologies used to deliver the end-to-end solution
"IS5"	this is HMG Information Assurance Standard No. 5 - Secure Sanitisation issued by CESG
"ISO/IEC 27001" "ISO 27001"	is the International Standard for Information Security Management Systems Requirements
"ISO/IEC 27002" "ISO 27002"	is the International Standard describing the Code of Practice for Information Security Controls.
"ISO 22301"	is the International Standard describing for Business Continuity
"IT Security Health Check" "Penetration Testing"	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
"Need-to-Know"	the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.
"OFFICIAL" "OFFICIAL-SENSITIVE"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services. the 'OFFICIAL–SENSITIVE' caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy.
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	the Security and Information Risk Advisor (SIRA) is a role defined under the CESG CESG Certified Professional Scheme

12.1. The Supplier shall comply with Departmental Security Standards for Suppliers which include but are not constrained to the following clauses. [12.2 – 12.24]

12.2. Where the Supplier will provide ICT products or Services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 25 September 2014, or any subsequent updated document, are mandated; that "contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme". The certification scope must be relevant to the services supplied to, or on behalf of, the Department.

12.3. The Supplier shall be able to demonstrate conformance to, and show evidence of such conformance to the ISO/IEC 27001 (Information Security Management Systems Requirements) standard, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

12.4. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data.

12.5. Departmental Data being handled in the course of providing the ICT solution or service must be segregated from other data on the Supplier's or sub-contractor's own IT equipment to both protect the Departmental Data and enable it to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Supplier and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 12.14.

12.6. The Supplier shall have in place and maintain physical security and entry control mechanisms (e.g. door access) to premises and sensitive areas and separate logical access controls (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.

12.7. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.

12.8. Any electronic transfer methods across public space or cyberspace, including third party provider networks must be protected via encryption which has been certified to a minimum of FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.

12.9. Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 12.10 and 12.11 below.

12.10. Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the Supplier or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to the Department.

12.11. All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the Supplier or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to the Department.

12.12. Whilst in the Supplier's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure waste paper organisation.

12.13. When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

12.14. At the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Supplier's ICT infrastructure must be securely sanitised or destroyed in accordance with the current HMG policy (HMG IS5) using a CESG approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Supplier or sub-contractor shall protect the Department's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

12.15. Access by Supplier or sub-contractor staff to Departmental Data shall be confined to those individuals who have a "need-to-know" and the appropriate level of security clearance, as required by the Department for those individuals whose access is essential for the purpose of their duties. All employees with direct or indirect access to Departmental Data must be subject to pre-employment checks equivalent to or higher than the Baseline Personnel Security Standard (BPSS).

12.16. All Supplier or sub-contractor employees who handle Departmental Data must have annual awareness training in protecting information.

12.17. The Supplier shall, as a minimum, have in place robust and ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might be, or could lead to, a disruption, loss, emergency or crisis. When a certificate is not available it shall be necessary to verify the ongoing effectiveness of the ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures, to the extent that the Supplier must have tested/exercised these plans within the last 12 months and produced a written report of the test/exercise, outcome and feedback, including required actions.

12.18. Any non-compliance with these Departmental Security Standards for Suppliers, or other Security Standards pertaining to the solution, or any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, shall be investigated immediately and escalated to the Department by a method agreed by both parties.

12.19. The Supplier shall ensure that any IT systems and hosting environments that are used to hold Departmental Data being handled, stored or processed in the course of providing this service shall be subject to an independent IT Health Check (ITHC) using a CESG approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

12.20. The Supplier or sub-contractors providing the service will provide the Department with full details of any actual storage outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management or support function from outside the UK. The Supplier or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Department.

12.21. The Department reserves the right to audit the Supplier or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Supplier's, and any sub-contractors, compliance with the clauses contained in this Section.

12.22. The Supplier shall contractually enforce all these Departmental Security Standards for Suppliers onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

12.23. The Supplier shall deliver ICT solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current CESG Information Assurance Policy Portfolio and Departmental Policy. The Supplier will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Supplier shall provide written evidence of:

- Existing security assurance for the services to be delivered, such as: PSN Compliance as a PSN Customer and/or as a PSN Service; CESG Tailored Assurance (CTAS); inclusion in the Common Criteria (CC) or CESG Product Assurance Schemes (CPA); ISO 27001 / 27002 or an equivalent industry level certification. Documented evidence of any existing security assurance or certification shall be required.
- Existing HMG security accreditations that are still valid including: details of the body awarding the accreditation; the scope of the accreditation; any caveats or restrictions to the accreditation;

the date awarded, plus a copy of the residual risk statement. Documented evidence of any existing security accreditation shall be required.

- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Supplier shall provide details of who the awarding body or organisation will be and date expected.

12.24. If no current security accreditation or assurance is held the Supplier and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Supplier and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation. This will include obtaining any necessary professional security resources required to support the Supplier's and sub-contractor's security assurance activities such as: a CESG Certified Cyber Security Consultancy (CCSC) or CESG Certified Professional (CCP) Security and Information Risk Advisor (SIRA).

13. Ownership of Rights in the Deliverables and the Specially Written Software

"Intellectual Property Rights"	means patents, trade marks, service marks, design rights (whether registerable or otherwise), applications for any of the foregoing, know-how, rights protecting databases, trade or business names and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom).
"Specially Written Software"	means any software written by or on behalf of the Supplier developed exclusively for the Department and supplied to the Department.
"Deliverable"	means non software content and materials exclusively delivered under this Contract including the collected or imported survey data, custom report templates, project cost models, user guide content ,manuals, survey data validation rules, and 3rd party system integration documentation.

The main deliverables include:

All the data fields created under section FR001

All the data validation rules created under section FR002

Any data connectivity specifically created with external datasets under section FR005

13.1 Title to and risk in any tangible property embodying the Deliverables and Specially Written Software shall vest in the Department upon acceptance.

13.2 Notwithstanding clause 13.1, the Department shall not acquire title to the Intellectual Property Rights in any Deliverables or in any Specially Written Software

13.3 In consideration of the payment of the relevant charges the Supplier hereby grants, or shall procure that the owner of the Intellectual Property Rights in the Deliverables and/or the Specially Written Software grants, to the Department, a non-exclusive licence to use, reproduce, modify, adapt and enhance the Deliverables and the Specially Written Software. Such licence shall be perpetual and irrevocable.

13.4 The Supplier shall supply the Department with a copy of the source code of any Specially Written Software for this Commission

13.5 The Department shall be entitled to engage a third party to use, reproduce, modify and enhance the Deliverables and the Specially Written Software on behalf of the Department provided that such third party shall have entered into a confidentiality undertaking with the Department for this Commission

14. Capital Assets – N/A

15. Welsh Language Scheme – N/A

16 Not used

17. Suppliers working on Department's premises- N/A

18. Suppliers co-operation with Departmental objectives

In performing the Contract, the Supplier shall at all times co-operate with the Department to maximise value for money, sustainable delivery where it is not detrimental to the interests of either Party to do so.

19. Sustainable Considerations – N/A

20. Suppliers use of sustainability impact assessment tools – N/A

21 Timber and products containing wood - N/A

22 Not used

23 Equality – already covered under FW 28 clause

24 Not used

25 Not used

26 Step In Rights N/A

27 SUPPLY CHAIN RIGHTS – N/A

28 TUPE – N/A

29 Safeguarding children and vulnerable adults – N/A

30 Supplier obligation to advertise sub-contracts – N/A

31 Apprenticeships N/A

32 Tax Compliance – N/A

33 Publicity

33.1 The Supplier shall undertake to make no reference to this Contract in any press releases, advertising or other promotional material before, during and termination of this Contract without the prior written consent of the Department except for information produced/published by the Supplier to exercise its legal obligations under this Contract

End of additional clauses

BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES to enter a legally binding contract with the Customer to provide the G-Cloud Services. The Parties hereby acknowledge and agree that they have read the Call-Off Terms and the Order Form and by signing below agree to be bound by the terms of this Call-Off Agreement.

For and on behalf of the Supplier:

Name and Title	Redacted
Position	CEO, Kykloud Ltd
Signature	
Date	19th August 2016

For and on behalf of the Customer:

Name and Title	Redacted
Position	Divisional Director of Capital Operations
Signature	
Date	19th Augsut 2016