Crown Commercial Service

G-Cloud 11 Call-Off Contract (version 4)

Contents

Part A - Order Form

Digital Marketplace service ID number:	8432 9995 8749 501
Call-Off Contract reference:	CQC ICTC 806
Call-Off Contract title:	Healthwatch CIVI CRM
Call-Off Contract description:	Hosting and maintenance of the Civi CRM and Web and Development of Web and CiviCRM products:
Start date:	01/10/2019
Expiry date:	31/03/2021
Call-Off Contract value:	£312,407.00 Including VAT
Charging method:	Invoice
Purchase order number:	275025629

This Order Form is issued under the G-Cloud 11 Framework Agreement (RM1557.11).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

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

From: the Buyer	Care Quality Commission on behalf of Healthwatch England Buyer's main address: 151 Buckingham Palace Road 3rd Floor London SW1W 9SZ

To: the Supplier	Circle Interactive Limited Supplier's address: 1 Osbourne Road Southville Bristol BS3 1PR England Company number: 05540067
Together: the 'Parties'	

Principal contact details

For the Buyer:	[redacted]
For the Supplier:	[redacted]

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 01/10/2019 and is valid for 18 months.
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for 1 period of 12 months, by giving the Supplier 3 months' written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 1 - Cloud hosting Lot 3 - Cloud support
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2, detailed in Schedule1 and outlined below: • Hosting and maintenance of Healthwatch England's Drupal based corporate websites, the CiviCRM website and 106 local CiviCRM sites; • Support of Drupal based corporate websites, 13 Drupal based website templates (potential growth to 148), CiviCRM and 106 CiviCRM instances (potential growth to 148) • Development of the Healthwatch England CiviCRM and 106 CiviCRM local sites (potential growth to 148 sites) • Development of the Healthwatch corporate websites and template - Incremental development of the Healthwatch England websites, local Healthwatch website template and integration options.
Additional Services:	Not Applicable
Location:	The Services will be delivered to Healthwatch England, 151 Buckingham Palace Road, 3rd Floor, London, SW1W 9SZ
Quality standards:	The Supplier will comply with any standards in the Call-Off Contract and Section 4 (How Services will be delivered) of the Framework Agreement, and with Good Industry Practice.
Technical standards:	The Supplier is to comply with all referenced technical standards provided by Healthwatch England in Schedule 1.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract is referenced in Schedule 1.
Onboarding:	Delivery and implementation to the requirements as specified in Schedule 1.
Offboarding:	The offboarding plan for this Call-Off Contract is specified in Schedule 1 under Section 9 Exit Management, page number 44-45.
Collaboration agreement:	Not Applicable
Limit on Parties'	The annual total liability of either Party for all Property defaults will not

liability:	exceed 125% of the total Call-Off Contract value. The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for all other defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance:	The insurance(s) required will be: ● A minimum insurance period of [redacted] following the expiration or Ending of this Call-Off Contract] ● Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity [redacted] for each individual claim or any higher limit the Buyer requires (and as required by Law) ● Employers' liability insurance with a minimum limit of [redacted] or any higher minimum limit required by Law ● Public Liability Insurance with a minimum limit of indemnity of [redacted] for each individual claim.
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 7 consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. The following audit clauses from the Framework Agreement shall apply: Clause 7.4 Clause 7.6 Clause 7.7 Clause 7.10
Buyer's responsibilities:	The Buyer is responsible for: The Buyer will assume project management responsibility for all works undertaken as part of this contract and will plan and attend regular contract management and service delivery meetings. The Buyer will ensure that throughout the duration of the contract all contracted parties will be subject to agreements that will ensure the necessary levels of support are met.

	Where necessary the Buyer will also ensure that processes and systems are put into place that promote efficiency and ensure effective delivery of requirements and parity between contracted parties. The Buyer retains responsibility for the roll out of software to its end users. Any delay in rollout will not affect pricing. The Supplier shall recommend applications, databases, operating system patches or upgrades which the Buyer will either approve or reject. If rejected, the Supplier will detail the impact on its ability to deliver the services. The Buyer will own and manage all specifications and approve or reject development subsequent to testing.
Buyer's equipment:	Not Applicable

Supplier's information

Subcontractors or partners:	Not Applicable

Call-Off Contract charges and payment

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

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

reference:	
Invoice frequency:	Invoice will be sent to the Buyer monthly
Call-Off Contract value:	The total value of this Call-Off Contract is: • £260,339.16 ex VAT (£312,407.00 Including VAT)
Call-Off Contract charges:	The breakdown of the Charges are specified in Schedule 2 and listed below [redacted] Costs include VAT and the total contract amount is £312,407

Additional Buyer terms

Performance of the service and deliverables:	Please refer to Schedule 1.
Guarantee:	Not Applicable
Warranties, representations:	In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants and represents to the Buyer that The Supplier will use the best applicable and available techniques and standards and will perform the Call-Off Contract with all reasonable care, skill and diligence, and according to Good Industry Practice. The Supplier warrants that all Supplier Staff assigned to the performance of the Services have the necessary qualifications, skills and experience for the proper performance of the Services.

	The Supplier represents and undertakes to the Buyer that each Deliverable will meet the Buyer's acceptance criteria, as defined in the Call-Off Contract Order Form. The Supplier undertakes to maintain any interface and interoperability between third-party software or Services and software or Services developed by the Supplier. The Supplier warrants that it has full capacity and authority and all necessary authorisations, consents, licences and permissions to perform the Call-Off Contract.
Supplemental requirements in addition to the Call-Off terms:	Not Applicable.
Alternative clauses:	Not Applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms:	Not Applicable.
Public Services Network (PSN):	Not Applicable.
Personal Data and Data Subjects:	Annex 1 of Schedule 7 applies.

1. Formation of contract

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

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

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

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

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.

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

Signed:	Supplier	Buyer
Name:	[redacted]	[redacted]
Title:		
Signature:	X	
Date:		

Schedule 1 – Services

healthwatch

CQC reference: CQC ICTC806

Healthwatch England Digital Systems: Hosting, Maintenance, Support and Development

Invitation to Tender

STATEMENT OF REQUIREMENTS

healthwatch

Contents

healthwatch

1 Executive Summary

1.1 About Healthwatch England

Healthwatch England is the national consumer champion in health and care. We have significant statutory powers to ensure the voice of the consumer is strengthened and heard by those who commission, deliver and regulate health and social care services. We are the national body for the local Healthwatch network of 148 sites across England.

Where very important issues arise, advice is provided to the Secretary of State for Health, the Care Quality Commission, NHS England, NHS Improvement or local authorities in England. By law they have to respond publicly to advice from Healthwatch England.

In order that we can deliver our statutory functions, we will be continuing to roll out our digital products to the local Healthwatch network and developing our understanding of how to use local insight credibly and with influence. This is how we plan to make sure that we improve the experiences of people using health and social care services.

The Healthwatch England business plan outlines 3 key priorities for 2019/20:

1. **Priority One:**
   Transform our communications with the public so more people can have their say.
2. **Priority Two:**
   Create tools to measure and improve the quality of Healthwatch and improve our impact.
3. **Priority Three:**
   Make evidence easier to access and ensure it's used by professionals.

1.2 Digital Outcomes

- To identify policies and programmes where Healthwatch evidence and insight can add value
- To see more partners using our insight and evidence to drive improvements in health and care
- To see an increase in public involvement in major health and social care reforms, ensuring that people's experiences and views help shape how health and care services work
- To facilitate the sharing of health and social care service information with Healthwatch England
- The use of a common system to capture systematic data within the network providing a high quality and consistent user experience

1.3 Business Objectives

- Align Healthwatch and CQC's Digital strategy
- Host, develop and continue to roll out our website and CRM for local Healthwatch and Healthwatch England
- Review and deliver ongoing CRM and website requirements throughout 2019-2021
- To put a single system in place for all local Healthwatch to enable them to capture patient experience feedback systematically
- To deliver a networkwide research programme to identify the digital needs of Healthwatch and build a corresponding digital development plan to improve our digital infrastructure.
- To deliver CRM training and support to the local Healthwatch network across 148 sites
- To make it easy for people to access national/local intelligence and reports

- To make it easier for people to find their local Healthwatch, share experiences and access advice and information content on-line
- To promote and maintain a consistent brand presence online

1.4 Digital Products

- CiviCRM – Healthwatch England site, demo, testing and staging sites plus (to date) 106 local sites[1]
- Feedback and Signposting Wizard
- Import functions
- Healthwatch England website, testing and staging sites
- Healthwatch Network website, testing and staging sites
- Local Healthwatch base website template[3], testing and staging sites
- Local Healthwatch websites (16 live, 15 in progress and 15 currently on a waiting list)[2]
- Healthwatch National Reports Library

1.5 Digital Users

The main users of the Healthwatch digital channels are the public, local Healthwatch staff including volunteers, and health and social care stakeholders. Healthwatch digital channels support the core business priorities in the following ways for the following users.

Priority	User	Role of digital	Current platform
1.Provide local Healthwatch with support	Local Healthwatch staff and volunteers	• Help discover and access advice, guidance, tools and training • Network on-line with other local Healthwatch securely • Secure system to capture and share patient experience and general workflow	Facebook Workplace[3] and a network support website CiviCRM
	Local Healthwatch Wider Public Local Healthwatch stakeholders	• Enable people to find local Healthwatch reports and news • Support a consistent brand experience • Enable people to get involved or share experiences • Enable people to access advice and information	Drupal[4] CiviCRM

[1] It is anticipated that more local sites will be installed in the near future so this number will increase. The ambition is that all 148 sites will adopt the same digital system to share information more effectively.
[2] The ambition is that more of the network will adopt the new website to help strengthen brand awareness, increase efficiencies across the network and ensure sites are being maintained in an appropriate way.
[3] We currently share resources with the network via Facebook Workplace designed to help local Healthwatch foster and build relationships online.
[4] We provide a Drupal website template which is being rolled out to the network with the potential for 148 local Healthwatch, this platform is maintained by Healthwatch England with regular updates.

2.Ensure peoples experiences help shape how health and care services work	Wider public, Health and care professionals, wider stakeholders	• Enable people to find national reports and news • Enable people to access advice and information • Enable people to share experiences • Enable people to find their local Healthwatch • Support a consistent brand experience	Drupal[5]

System	Platform and service	Customer
Healthwatch England website Healthwatch Network website	Drupal used by all Drupal	Public and professionals Healthwatch staff and volunteer
Local Healthwatch websites	Hosting maintenance and support only of HWE site and x31 LHW sites	Over 30 have or are in the process of moving across to the new site, with another 15 or have so far expressed an interest in our new offer which is currently being piloted. We plan on having 50 by the end of the financial year 19/20.
Healthwatch England CRM Local Healthwatch CRM	Drupal used by all. Hosting maintenance and support provided to all.	Two thirds of local Healthwatch use the system
Online networking	Facebook Workplace	900+ users have access

2 The Requirement

Healthwatch England requires a suite of digital resources which include hosting, maintenance, day to day support as well as development and training support. This will enable Healthwatch to continue to discharge its statutory functions, primarily the sharing of information gathered from the local Healthwatch network about people's experiences of health and care services.

The requirement has been divided into five individual lots that can be bid for individually or as a whole and can be summarised as follows:

Lot One	**Hosting and maintenance of:** • Drupal based corporate websites and local sites (potential growth to 148), • CiviCRM website and 106 CiviCRM local sites (potential growth to 148)
Lot Two	**Support for** Drupal based corporate websites: • 16 Drupal based local sites (potential growth to 148), • CiviCRM and 106 CiviCRM instances (potential growth to 148)
Lot Three	**Development of** CiviCRM website and 106 CiviCRM local sites (potential growth to 148)
Lot Four	**Training for** CiviCRM Users
Lot Five	**Development of** Healthwatch corporate websites and local base site and roll out of development updates.

Each of the five lots are outlined in more detail below:

Lot One	**2.1 Hosting and maintenance of Healthwatch England's Drupal based corporate websites, the CiviCRM website and 106 local CiviCRM sites**

- Healthwatch England requires an infrastructure that can host up to 160 CRM sites; this includes staging and demo sites, the Healthwatch England CRM site and the Staff and volunteer resources site as well as the option to host directly with the local Healthwatch sites.
- Hosting is also required for the Healthwatch corporate websites to include but not restricted to Healthwatch England website, Healthwatch Network the local Healthwatch base website, including staging and test sites for all. Hosting is also required for up to 148 local versions of the base site.
- In terms of the required CiviCRM maintenance the supplier will need to outline how (and

where necessary in collaboration with developers) they will work to ensure that the following requirements can be delivered successfully:
Maintenance and upgrades including:
- security releases
- annual penetration testing
- patch testing
- porting
- back ups
- disaster recovery
- manual changes
- rolling out changes to the network
- upgrades and maintenance of all sites
- automated selenium tests
- visual testing

- In terms of the maintenance requirement for the corporate website the supplier will need to outline how (and where necessary in collaboration with developers) they will work to ensure that the following requirements can be delivered successfully:
  - annual penetration testing
  - patch testing
  - daily back-ups
  - deployment of security updates when necessary.
- Healthwatch England will require continued rollout of the CiviCRM to the network, ensuring that a site can be rolled out within 72 hours of confirmation.
- Healthwatch England will also require continued setup and rollout of the local Healthwatch sites on a batch basis.
- The current system is hosted by an independent provider. All bids should include information on how the supplier will work with the existing incumbents to maximise on any efficiencies that can be obtained from this arrangement.
- Rollout of the Healthwatch England base website requires a separate contracting arrangement between the supplier and local Healthwatch organisations in order to carry out the website services. Healthwatch England is anticipated to roll out 50 base sites during financial year 19/20. There is potential to have 148 sites in total.

Lot Two	**2.2 Drupal based corporate websites, 13 Drupal based website templates (potential growth to 148), CiviCRM and 106 CiviCRM instances (potential growth to 148)**

- Healthwatch England requires technical support for 106 CiviCRM (potential growth to 148) sites amounting to 4 days per month. The supplier must provide:
  - a ticketing system to enable the local Healthwatch network to raise issues
  - a system that enables the resolution to all raised issues within 48 hours
  - technical support and advice
  - basic support and system tracking

- rolling out new sites within 24 hours
- bulk email rollout to the network
- monitoring of data push systems
- failure management and resolution

- Healthwatch England also requires CiviCRM and web consultancy up to 6 days per month which includes:
  - project management and forward planning
  - planning roll outs and technical developments
  - meeting attendance
- The CiviCRM requirement also includes management of the CiviCRM "data push" functions. This enables Healthwatch England to pull data through from network users automatically at a rate of 2 activities per second.
- Healthwatch England offers a website template to the network. Currently 16 Healthwatch are using this with a total of 50 planned for the end of March 2020. This has the potential to increase to 148 sites. The supplier must provide:
  - a ticketing system to enable the local Healthwatch to raise issues
  - a system that enables the resolution to all raised issues within 48 hours
  - technical support and advice
  - basic support and system tracking
  - batch rolling out new sites agreed with our teams
  - failure management and resolution
- The supplier must guarantee system security for users including a password dissemination process and ensuring all relevant security protocols are in place.

Lot Three	**2.3 Development of the Healthwatch England CiviCRM and 106 CiviCRM local sites (potential growth to 148 sites)** (Development will be planned and prioritised according to the Healthwatch England Strategy which is currently in production)

- Healthwatch England provides a system that ensures data transfer compatibility if either the core system changes or local Healthwatch providers opt for another system other than the Healthwatch England CiviCRM.
- Discovery, development and deployment of system improvement in support of the Healthwatch England business plan and strategy. Working with local Healthwatch to:
  - Develop an expert understanding of Healthwatch users' digital needs
  - Engage with users and stakeholders through a range of channels to ensure future take-up and use of digital products
  - Carrying out user research across the network
  - Analysing the results of the research and producing a clear and thorough action plan
  - Help define, explain and iterate a product vision that is compelling to Healthwatch users, our team and our stakeholders
- Ongoing improvement of the CiviCRM system including the implementation of ad-hoc, small scale pieces of development. This will include:

- ongoing refinement and development of the Healthwatch England CiviCRM taxonomy
- progressing work undertaken on the analytical functions within CiviCRM
- improving the user experience of the CiviCRM system
- Improvements to import functions

- Development testing on staging sites with well-planned staggered deployment to minimise impact upon users and highlight hidden bugs before full rollout.
- Discovery and development work to assist in integrating Healthwatch digital communications channels – see Lot Five

Lot Four	**2.4 Training for CiviCRM users** Healthwatch England will support the local Healthwatch network by providing a range of user training that has maximum reach and increases usage of the CiviCRM. It must be based upon a process of ongoing feedback and review

- The Healthwatch England training requirement includes the development and delivery of a suite of resources as follows:
  - the delivery of 27 CiviCRM training sessions. This will include new user training as well as refresher training. The delivery method will be dependent upon the training needs requirement but will include a range of face-to-face sessions across England, hosting webinars on specific subjects and ad hoc training for other digital systems if required.
  - 18 days for the development and production of user guidance to support Healthwatch England digital systems these will include the development and production of accompanying training videos and pdf guides.
  - Three days support and training for survey production and engagement
  - Three days of telephone support.
- As a minimum CiviCRM user training sessions will need to include;
  - Introduction to the CiviCRM for new users.
  - Reports.
  - Contacts.
  - Groups.
  - Relationships.
  - Activities.
  - Data Protection.
  - Searching & Exporting.
  - Events.
  - Case Management.
  - Using the Enquiry Feedback Wizard.
  - Using the Import Functions.
- The trainer will ensure that any intelligence received on system usage and functionality will be fed back into the Digital Team at Healthwatch England to inform system development.
- The trainer will advise trained users on how to effectively cascade their learning to use it to maximise efficiencies.
- To provide a train the trainer function for Healthwatch staff.

- To attend the Healthwatch Annual Conference in support of CiviCRM users.
- To attend CiviCRM development meetings when and if required.

Lot Five	**2.5 Development of the Healthwatch corporate websites and template** Incremental development of the Healthwatch England websites, local Healthwatch website template and integration options.

Incremental development of the Healthwatch England websites and the template for local Healthwatch:

We currently maintain a national website and a staff website that is on a subdomain. We also develop and maintain a base site, that's replicated for local Healthwatch. This is hosted by our own supplier to allow for future updates to be rolled out centrally.

Our work includes but is not limited to:

- Ongoing improvement and developments to the main sites and base site including:
    - Updates to code
    - Updates to content (media files and content)

- Continued development and refinement of the National Reports Library. The National Reports Library contains all reports from across the Healthwatch network. The work will cover but is not limited to:
    - How information is displayed
    - Reports library taxonomy
    - Information structure and connectivity
    - Enhanced search
- Making sure all site development and non-functional requirements will need to be accessible for those using screen readers and comply with our accessibility guidelines (accessible at http://www.healthwatch.co.uk/website-accessibility) and W3C standards.

The following projects have the potential to be commissioned and developed:

- Exploring functional development of Healthwatch England main website and local Healthwatch template such as integration with the local Healthwatch CiviCRM covering:
    - events promotion and sign-up.
    - CRM mailing sign-up.
    - surveys.
- Development and refinement of an online ticketing and performance tracking system to enable Healthwatch England to track its support requests and offering. Data from this system can be exported in a CiviCRM acceptable format to be available for import.
- Development or integration of a feedback centre to allow for the public to share their experiences of UK health and care services.

healthwatch

2.6 General Requirement: Transition In and Transition Out

All prospective suppliers are required to outline their ability to provide the following where applicable as part of their entry and exit arrangements:

2.6.1 System Migration

- A process outlining migration to a new system including preparing handover notes of system customisations, modules and extensions.
- Working documents including specifications, wireframes and sign off sheets.
- Access to any project tools in place, i.e. Basecamp, or migrate all data over to a new project tool.
- Access to any code that has been used.
- Full access to all servers, detailed instructions of how the servers have been configured and migration of data in existing servers (if relevant).
- Full access to any tooling or monitoring used to deploy or test the infrastructure.
- Detailed information about the development build and how it would impact on any new system migration.
- A project plan for the migration to a new system which includes data transfer, both for Healthwatch England and Local Healthwatch.
- A process to ensure minimal system downtime for migration to a new supplier, if any.

2.6.2 Data Transfer

Should Healthwatch adopt any new system within scope of the contract the supplier will need to facilitate any necessary data transfer ensuring minimum disruption to the ongoing work of local Healthwatch and Healthwatch England. All potential suppliers will need to describe how they will ensure the provision of:

- Full access to the databases and data to enable transfer from the current system into any new system, if required.
- An outline plan that ensures continuity of data with minimum disruption to the site and to the ongoing work of local Healthwatch and Healthwatch England, if required.
- The means to map data from the existing system to the new system providing database exports if necessary.
- A project plan which includes a timeline to undertake a complete exit from the current CiviCRM system to a CQC approved system, if required.
- A clear process by which they will work with the CQC technical team, as well as Healthwatch England to achieve any transition.

2.6.3 Data Security and Privacy

- An outline on how the supplier will destroy and remove sensitive information from all media, ensuring it is not disclosed to other individuals or organisations.

3 Background to the Requirement

3.1 The CiviCRM Project

The Customer Relationship Management (CRM) project was initiated in 2012. Following evaluation, the CiviCRM system was chosen by Healthwatch England for the following reasons:

- It is flexible
- It is secure
- It is an open source, web-based system
- And has been developed for non-profit and third sector organisations.

The aim of the project was and continues to be the provision of a CRM system that supports the common requirements of 148 local Healthwatch, whilst providing sufficient local customisation to accommodate each organisation's distinctiveness in approach and process.

Initially there was a pilot group of 33 local Healthwatch sites. Due to the way the project was originally set up, Healthwatch had been effectively running two separate projects; the pilot project and the rollout project.

The pilot project is distinct in that they were able to make field changes on the system that led to significant variation between sites. Subsequently the fields were locked down for the rollout project. The variation in fields caused issues including upgrades crashing, and difficulty in installing developments to the affected sites. This has been rectified in all but a few cases and Healthwatch have now rolled out the Enquiry Feedback wizard to improve the user experience and simplify inputting (where local Healthwatch capture their consumer feedback data via a webform that is then forwarded to Healthwatch England).

In September 2015 Healthwatch completed the pilot phase and rolled out the system to a further 44 local Healthwatch (as per an agreement with the Department of Health), this constituted the "rollout phase". Healthwatch then spent 18 months standardising the pilot sites and the rollout sites, changing altered fields back to the agreed common base, undertaking further site development and mapping across the field changes. Most users have now moved onto the standardised system with only one or two users still using their initial fields and not taking up the Enquiry Feedback Wizard. We currently have 106 instances rolled out, equating to around 600 users.

Purpose	To provide local Healthwatch and Healthwatch England with a CRM system to enable them to capture and share patient experience feedback in a systematic way.
Primary Users	Local Healthwatch and Healthwatch England
Benefits of the CiviCRM	• It is a secure portal to capture data in a systematic way. • User access is restricted and the system is tested annually for security and cyber-attacks to ensure robustness. • Provides local Healthwatch with a secure operations tool for managing day-to-day workflow and capturing consumer experience, which they do as part of their role to ensure any risks to consumers of health and social care services are highlighted. • Pushes intelligence from each local site through to Healthwatch England via the 'data push' system (see detail below) which informs on trends and themes in health and social care at a local level as well as engagement work being undertaken locally. • Users can manage and report on contacts, enquiries, signposting and case information securely, manage meetings, face to face engagement and consumer experiences. • The system also enables them to produce surveys and newsletters, manage and measure the impact of activities and events as well as report on meeting attendance.
Where we are now – business utilisation	
• Capturing the various relationships that the local Healthwatch network may have with a member of the public or health/social care organisation. As an example, the interaction a consumer has had with a GP and with a hospital service. • Linking the relationships between consumers as individuals, groups and organisations. As an example, the ability to link organisations or groups together. • Creating and storing contact data; these contacts are both organisations and individuals. The data can include items such as addresses, websites, telephone numbers. • Any activities that have taken place: from each activity follow up activities can be scheduled, and files attached as necessary. • Sending communications, either bulk emails or single communications to specific contacts; scheduled reminders can also be set so that an email is automatically sent to an assigned user to follow an activity. • Case management; allowing users to create, manage and track workflows. • Reporting; allowing users to run and save reports, export, download and add to case	

management, create templates and automate. Reports most commonly used by local Healthwatch are those within Enquiry feedback, as well as the Enter and View reports and Annual Reports Other reports required could be research on Health and Care services, statements on quality accounts, intelligence and engagement reporting for CCG's. Report templates would need to be built for the most common reports used across the network.

- The Enquiry/Feedback Wizard is used to record consumer feedback that the local Healthwatch collects and sends it through to Healthwatch England CiviCRM. The system automatically creates a case on the client side and sends the data through to the Healthwatch England CiviCRM via the Data Push function. The data enters a queue to be checked by Healthwatch England staff.
- The Import functions are built into the Healthwatch England CiviCRM and is used by those local Healthwatch that do not utilise a standalone instance of the CiviCRM. This system allows for consumer feedback to be uploaded directly to Healthwatch England CiviCRM via a CSV file where it enters a queue for Healthwatch England staff to check.
- The ability to carry out outbound communications and campaigns to a targeted audience for marketing and stakeholder management purposes, this would include sending newsletters and calls for action.
- Event management; to create events, record and manage the event host and attendees.
- The ability to conduct effective and meaningful market analysis based on the information captured.
- Local Healthwatch CiviCRM Data Push functions – a function to pull through activities from the local Healthwatch Enquiry Feedback area of the local sites through to the Healthwatch England site at a rate of two activities per second.
- Data Push Import Functions – two import functions for users that do not currently have the CiviCRM. This allows local Healthwatch to send data to the Healthwatch England CiviCRM via data uploads from CSV spreadsheets.
- Local Healthwatch tab – To create a separate tab to enable local Healthwatch to create fields and options that do not overlap with the Enquiry Feedback area of the system, that will allow users to capture local information required that does not need to be standardised with other network users or pulled through to the England site via the Data Push.

Where we want to get to

- Year-end reviews of Healthwatch England's taxonomy and alignment of any changes across the network within their Enquiry Feedback areas so Healthwatch England can pull through the correct data.
- Annual Penetration testing, to ensure robustness of the system in conjunction with external supplier.
- Undertaking various national workshops on issues including the integration of data

capture, linking county users together to form "devolved ways of working with the CRM", attending training workshops, Healthwatch conferences and CRM Stakeholder Groups when necessary

- Delivering up to 27 new user training sessions per annum including bespoke sessions and improved induction training to increase usage and encourage future system development. Improving and developing webinar-based training to increase the number of Healthwatch reached, provide more flexible, shorter sessions in the work place.
- Production of new support materials for our digital resources to support a network support communications plan.
- Data governance. Ensuring that data entered into the CRM and pulled through via the data push is accurate, high quality data.
- Data security and data protection training.
- Implementing ad-hoc pieces of development work following feedback from CRM Trainer and/or CRM Stakeholder Group
- CRM integration to website and local Healthwatch website template.
- Fed through the Digital Transformation/Discovery project new innovative plan to meet the digital needs of the Healthwatch network resulting in maximum adoption from the network to our digital offering.

3.2 Corporate Websites Project: (1) Healthwatch Websites

The Healthwatch England website and local Healthwatch website templates were developed to:

- Promote and maintain the Healthwatch brand presence online.
- Make it easy for the public and stakeholders to access national/local intelligence and reports.
- Make it easy for people to find their local Healthwatch, share their experiences and be signposted to services

The key deliverables of the project included:

1. Improved navigation to help people find what they are looking for as well as improved brand representation
2. Improving usability, making the sites easier to use and access ensuring that the design makes the content engaging and useful
3. Increasing responsiveness, enabling access using different devices and providing a template that can be incorporated as part of the CRM offer
4. Improving efficiency by enabling updates to be rolled out across the sites and ensuring a good level of security.

Purpose	1. Maintain a website template for local Healthwatch and evolve the Healthwatch England website(s) so that they that they respond to changes in technology and meet user requirements. 2. To explore potential integrations with the Healthwatch CRM and

	the provision of a closed community where local Healthwatch can network.
Primary Users	The public and stakeholders

Where we are now

Healthwatch websites and base website

- Our sites are now responsive.
- We have a new staff section website on a subdomain for local Healthwatch staff and volunteers to access support information.
- The current template and that used by local Healthwatch is based on Drupal 7.
- Both websites include improved navigation on both local Healthwatch websites and Healthwatch England's allows users to find information quickly or easily.
- We are in the process of rolling out the base website in batches to the local Healthwatch network. It is anticipated we will have 50 base sites be the end of the financial year 19/20, with a potential to have 148 sites in total. Each base site requiring a separate contracting arrangement between the supplier and local Healthwatch organisations in order to carry out the website services.

Where we want to be in the future

- Healthwatch England needs to continue its development of its online space that clearly brings together the support and resources that are provided to the local Healthwatch network including:
  - CRM
  - Facebook Workplace
  - Communications Centre
  - Guidance and support documents
  - Training
  - News
- Continued batched rollout out of the local Healthwatch website template with the potential for 148 sites.
- Continued work to ensure that our websites respond to new user requirements and are accessible to all to ensure that everyone has a good user experience. To roll out updates of any digital updates across the Healthwatch digital website estate
- A process/facility for Healthwatch England to automatically populate local sites with content updates. These will include image library content, tagged news, tagged event items and pages to the website templates to support content refreshing to the whole network.
- A support portal and performance tracking system via an "online ticketing system" to allow for a range of information and support requests from Healthwatch England

stakeholders. The system would also allow for Healthwatch England to track its support requests and track performance and should be adaptable to changing needs.

- National Reports Library – continued development and refinement of this system based on user feedback of the service and Healthwatch England needs. Supporting local Healthwatch to enable manage their own reports on the library.

4 Service Levels and Non-Functional Requirements

4.1 Availability Requirements and Support

4.1.2 Any system is required to meet service availability levels of 99.5% Monday to Friday 5 days a week with the exception of bank holidays. System maintenance should be carried out outside those working hours.

4.1.3 The following server environments are required Live, Test, Development, User Acceptance Testing, Pre-production and Training, if appropriate to the nature of the service.

4.1.4 System will be supported in the event of a disaster and any recovery plans will be tailored to Healthwatch England needs and be compliant with business continuity standards.

4.2 Recovery Time

4.2.1 The recovery mechanisms must support minimal recovery time with optimal recovery points.

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

4.3 Performance and Scalability

4.3.1. The system must handle an increase in storage requirements without major system changes or data migration activities.

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

4.3.3 The system must minimise the load on Healthwatch England's network and provide mechanisms for reporting on and controlling that load.

4.3.4 The system should be performance tested so that performance at the time of commissioning can be accurately known

4.3.5 Response times for the website should be in line with NHS Digital standards (for example current home page size 1.8MB to load <1.7s). A typical task in the CRM should be performed at more than 2 activities per second.

4.4 Integration

4.4.1 System should seek to support authentication using Healthwatch England's existing staff directory service and seek to implement a suitable single sign on (SSO).

4.4.2 Where relevant to its function, CiviCRM and Drupal will be capable of interfacing with Healthwatch England internal and external data sources, such as Microsoft Access and Excel, Sharepoint and Facebook Workplace, MySql, and potentially SQLServer 2008 and above. A service oriented approach should be used, where practical and possible.

4.4.3 System shall support the use of a range of mobile devices, meeting CESG requirements.

4.5 Monitoring

4.5.1 The application must be monitored by the provider, with suitable alerting tools in place to notify of current or imminent service breaches and security issues.

4.6 Reporting

4.6.1 The Contractor will submit service availability report on a monthly basis.

4.6.2 The Contractor will submit a monthly reporting on current versus projected capacity, both in terms of storage and licenses.

4.6.3 The Contractor will provide a monthly report on the overall performance on the service, including performance, requests and incidents relating to the service.

4.7 Change Management and Release Process

4.7.1 The Contractor will demonstrate their ability to perform changes to the application in a controlled and structured manner, including adherence to any methodologies.

4.7.2 System to be subject to formal processes for release management, in association with customer with regard to testing.

4.7.3 Responsibilities related to program coding, application testing and approval, program transfer between environments are segregated.

4.8 Usability

4.8.1 The application must support UK English.

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

4.8.2 The solution must provide an intuitive user interface that enables the user to complete a task whilst minimising the need to navigate the system

4.8.3 Customer Desktop devices are restricted in terms of the ability to download components from external sources. The system shall operate with the minimal need for software components to be applied to PC or desktop devices. The standard desktop is Windows 7 32 bit with 3.5 Gb of RAM with Internet Explorer 11 and Microsoft Office 2010. In the future windows 10 and/or a 64 bit

client may be used and any client software should be able to take advantage of that and increased memory availability.

The supplier must provide comprehensive systems administration, installation guides and processes, as appropriate to the nature of the service.

A complete, typical deployment architecture must be described.

4.9 Compliance

4.9.1 The application must comply with the CQC Architecture Principles.

4.9.2 Compliance to all U.K. legal requirements including the Data Protection Act (1998), the Freedom of Information Act (2001) & Privacy laws.

4.9.3 The system or service must comply with the U.K. Government Digital strategy.

4.9.4 There should be a mechanism for purging and archiving data in accordance with an agreed data retention policy.

4.10 Escrow

4.10.1 In the event of buyout or liquidation of the vendor the base source code of the software must be made available to Healthwatch England.

4.11 Support

4.11.1 Supplier shall provide a service desk with the ability to log and resolve incidents and requests. The supplier shall provide a named contact for escalation of issues and regular interface between the supplier and the customer. The supplier shall detail the channels available and typical response times for both fault resolution and functional query support. Support levels are further detailed in sections 4.13 and 4.14.

4.12 Accessibility

4.12.1 The system shall enable accessibility via assistive technology for those who cannot use a standard mouse and/or keyboard e.g. WA3, Dragon Naturally Speaking and Windows 7 Voice Recognition software. It shall also enable access for those with additional visual or hearing needs. The supplier shall state how these needs are met by the software.

4.13 Service Hours

4.13.1 Service Hours are the times when users can expect to access and use the full functionality of the CRM and/or Web publishing systems. Service Hours are 24 x 365 and is comprised of Core Hours and All Other Hours:

4.13.1.1 Core Hours:	08:00 to 20:00 Monday to Friday excluding Bank Holidays
4.13.1.2 All Other Hours:	all times other than Core Hours

4.13.2 Support Hours are the times during which the Contractor will provide resource to respond to and resolve incidents and requests associated with the CRM and/or website. Support Hours are 08:00 to 20:00 Monday to Friday excluding Bank Holidays.

4.13.3 CRM and website availability will be measured against Service Hours and presented as separate percent values

Period	Hours	Target Availability	Maximum Outage
Production environments			
Core hours	08:00 to 20:00 Mon to Fri	99.5%	4 hours
All other hours		99.0%	4 hours
Non-production Environments			
Core hours	08:00 to 20:00 Mon to Fri	97%	24 hours
All other hours		95%	24 hours

4.13.3.1 The minimum availability will be measured across a 13 week rolling period.

4.13.4 The maximum allowable outage is the maximum the CRM and/or website can be unavailable to the users. The Contractor will inform the Authority within eight (8) Working Days of its intention to carry out the planned maintenance that will require more than two (2) hours of downtime during the "all other hours period". Where the Authority's is withheld (which shall not be unreasonable) both parties will enter into negotiations in good faith to resolve the issue.

4.13.5 The Core Hours availability target for the production environment will be subject to Service Credits.

4.14 Incident Resolution

Will be according to the severity within the times stated in the following table:

Category	Description	Response Time	Resolution Time	Hours of Cover
Severity 1	Entire system unavailable to all users	15 minutes	4 Hours	08:00-20:00 Mon-Fri exc. Public Holidays
Severity 2	Specific modules of system unavailable to all users	30 minutes	8 Hours	08:00-20:00 Mon-Fri exc. Public Holidays
Severity 3	Severe functionality defect	1 hour	12 Hours	08:00-20:00 Mon-Fri exc. Public Holidays
Severity 4	Minor functionality defect	1 hour	Scheduled outage to resolve	08:00-20:00 Mon-Fri exc. Public Holidays

4.14.1 Resolution time is time between detection of the incident, by monitoring and alerting systems or a report to the Contractor helpdesk, and restoration of the functionality to normal operating performance levels.

4.14.2 The Contractor Help Desk will be available to received incidents and requests 24 x 365

4.14.3 In the event of Severity 1 incidents, the Contractor shall inform the appropriate Authority contact as identified in the following table in line with the times indicated.

4.14.4 Core Hours; contact by telephone and email

4.14.5 All Other Hours; contact by text and email supplemented with telephone at beginning of next Core Hour day.

Service downtime that will impact availability during core hours	Authority	Contractor
Less than one hour	Digital Systems Development Manager	Service Manager
More than one hour	Head of Intelligence and Analytics	Service Delivery Manager
More than four hours	Deputy Director	Service Delivery Manager
More than eight hours	National Director	Contractor Client Director

5 Functional Requirements

5.1 Users and Instances

The Contractor should assume the following maximum number of Users and instances:

5.1.2 CRM is currently 106 sites with approximately 600 users. The solution (see section 5.3 for core requirements) will be scalable to meet potential demand for 160 sites.

5.1.3 The website solution (see section 5.4 for core requirements) will meet the needs of the main Healthwatch England website as well as provision for up to 160 Local Healthwatch sites.

Based on the following assumptions:

5.2 Assumptions

The contractor will ensure that:

5.2.1 The system may be enhanced through a series of releases to meet additional requirements over time and some of those may supersede those listed; such requirements, as agreed by the Contractor, shall be added via the change control process as stated in the contract schedules.

5.2.2 The system is currently delivered through a mix of standard CiviCRM and Drupal functionality and configuration of CiviCRM and Drupal, and the contractor is not responsible for issues that arise from the capabilities of the standard product of either.

5.2.3 The Contractor is only responsible for delivering the Services listed in sections 5.3 and 5.4. The parties agree that the system meets the core requirement and process requirements at the commencement of this contract. The listed core requirements in sections 5.3 and 5.4 will be met and continue to be met by the release requirements as requested by the Authority and as agreed by the Contractor providing that this is within the parameters of the CiviCRM and Drupal products.

Following a new release that, by agreement with the Authority, changes functionality so that a Core Requirement cannot be met, the Contractor shall not be liable for a failure to meet the Core Requirement. Following a change to the CiviCRM or Drupal standard product that means a Core Requirement can no longer be met, the Contractor shall not be liable for a failure to meet that Core Requirement.

5.3 Core Requirements - CRM

5.3.1 The system will have the ability to record all of the external organisations and contacts with which the Authority deals.

5.3.2 The system will have the capability of recording relationships between organisations and contacts.

5.3.3. The system will enable the maintenance of a complete history of all tasks and interactions by organisation and contact.

5.3.4 A dashboard view will be provided to give a summarised view of information held about an organisation to the Users of the System, with more information on any kind of the items available via drill down.

5.3.5 The system will support the creation of activities which support specific business processes. The types of activity carried out by the system, along with the associated tasks, are to be defined by the Authority. The overall process for this is as follows:

5.3.5.1 Activity is created and the detailed tasks to be performed are created for the activity.

5.3.5.2 Resources are assigned to the individual tasks

5.3.5.3 Tasks are completed and marked as complete

5.3.5.4 Exception reporting occurs for uncompleted tasks

5.3.5.5 More complex activities may have further child activities, creating a hierarchy.

5.3.6 Task plans (a predefined set of tasks) will be used to ensure that a consistent, standardised approach is used for all activities of a certain type. However, it should also be possible to modify the default list of tasks for a particular activity. The task plans will allow the skills required to perform a particular task to be defined. Definition of the content of the task plans and associated tasks is an Authority responsibility. The System will provide an administration capability for such tasks and task plans. Users will then be able to modify the detail of individual tasks.

5.3.7 Enquiry/Feedback activity is used to log external feedback into the organisation that needs to be managed through a lifecycle of reporting, feedback and resolution.

5.3.8 The system will support generic query handling

5.3.9 The Authority deals with correspondence received via a number of different channels and users will be able to record all such interaction with contacts.

5.3.10 The users will have a mechanism to be able to send correspondence to contacts and to record the fact that such correspondence has been sent. This may be across a variety of channels and may be target at individuals, or at large groups of people.

5.3.11 The system will handle the following inbound channels:

- Telephone
- Email
- Printed mail
- In person
- Via Social Media
- Web Form
- Other – ability to add

5.3.12 It will be possible to create e-mails and letters using standard templates from inside the system, in which case the interaction should be automatically created and attached to the relevant contact. Definition and administration of templates will be a responsibility of the Authority.

5.3.13 It will be possible to attach documents (e.g. Microsoft Word, scanned image, PDFs) to contacts, cases and activities.

5.3.14 It will be possible for users of speech recognition software to use agreed parts of the system and to achieve the same functional results as users of the normal high interactivity interface.

5.3.15 It will be possible to record changes to named fields in the audit log. Definition of the writes and reads to be recorded in the audit log will be the responsibility of the Authority.

5.3.16 It will be possible to enforce password strength rules in accordance with the guidelines previously provided by the Authority. Any new rules or guidelines will be added via Change control.

5.3.17 It will be possible to review and where necessary delete attachments against a retention schedule whilst keeping an audit of the attachment deleted. Definition of the retention schedule will be the responsibility of the Authority.

5.3.18 The system will enable the production of a number of static and ad-hoc reports. The reports may be delivered using a combination of predefined queries, manually entered queries, or CiviCRM inbuilt reporting functionality.

5.3.19 The system will be capable of producing output, in a format to be agreed, to allow for interface with the Authority's intelligence systems, and of accepting information, in a format to be agreed, from the Authority's intelligence systems.

5.3.20 The system will be capable of interfacing with web-based forms, via the Authority's website and associated web applications.

5.3.21 The system will be capable of loading new contact, case or organisation datasets, in a format to be agreed.

5.3.22 The system will be capable of maintaining an audit trail to allow the identification of user name, date and time of all amendments and deletions of data entries. The audit trail can be retained for a period of up to six (6) years. The administration of this is the responsibility of the Authority.

5.3.23 The system will permit and organisation to be linked to any other organisation, and any contact to any organisation. It will be the responsibility of the Authority to ensure that the relationships defined make business sense.

5.3.23.1 For each relationship, a relationship type and/or comment will be captured.

5.3.23.2 The relationships between organisations will be easily navigable

5.3.24 A dashboard view is required to provide a single summarised view of information held about an organisation. This may involve the development of a number of separate dashboard views, each pertinent to a different user role or instance of the system (for example, local version of CRM). The system will support the merging of organisations and allow users to see history of each old organisation.

5.3.25 Activities will be manually created in the System. These can be scheduled to take place at any time in the future, with a specific start date, due date and end date. Assigning a task plan to an activity will generate a default set of tasks for the activity. Individual tasks can also have start and due dates.

5.3.26 The system will make it clear to an employee (User) that they have been assigned to a task or an activity.

5.3.27 The system will support a process to define and maintain employees.

5.3.28 The system will support creating a new contact if the contact does not already exist within the system and linking that new contact to an organisation, if applicable.

5.3.29 The system will allow the acceptance of inbound communication from multiple channels. Inbound communications will require a Service Request (SR) to be created. The system will allow the processing of SRs through a defined lifecycle from creation to resolution. An SR will pass through various statuses during its lifetime. The system will not enforce which transition states are allowed. Typical sequence might be:

- Open
- On hold
- Pending
- Overdue
- Closed
- Resolved

5.3.30 The system will enable associating tasks to the SR to record the detail of internal actions performed and correspondence sent/received.

5.3.31 The system will allow the passing of SRs between employees/teams for resolution. For SRs assigned that have been assigned to a particular team or individual, the assignees will be able to access and manage this queue of work.

5.4 Core Requirements - Website

The website needs to supply a common set of tools that offer enough autonomy for both Healthwatch England and for each Local Healthwatch to use to support their own specific user needs and preferences.

5.4.1 The site will provide the ability to publish all content required in support of Healthwatch England and Local Healthwatch.

5.4.2 The site will be structured to ensure Search Engine Optimisation (SEO)

5.4.3 The site must incorporate flexibility in navigation to accommodate for potential overhaul of organisational structures, taxonomies, and roles and relationships

5.4.4 The site administrators/editors must be able to easily organise the non-locked down navigational structure of the site, adding, deleting and amending sections and pages via the content management system (CMS)

5.4.5 Site administrators must be able to perform spell check and grammar check.

5.4.6 The site will contain a glossary of terms and acronyms and for these glossary terms to be linked to via site content

5.4.7 The site will have the ability to metadata tag.

5.4.8 The site will provide a directory service, singling out the relevant contact person for each stakeholder on a particular piece of content.

5.4.9 The site will have the ability for site administrator to create, edit and delete users and groups, including batch upload of new accounts

5.4.10 The site should function as a central method of distributing news and messages to stakeholders and other groups. Users should have role-based access so that news, policies, etc. can be targeted at them. Content should also be made available via groups.

5.4.11 The site will allow for the ability to publish text via a WYSIWIG editor. Content editors should not need recourse to knowledge of HTML. The site will also allow for the embedding of multimedia (typically photos, videos, slideshows and audio files) as well as linking to internal and external resources.

5.4.12 The site will allow for the uploading and publishing of standard format documents (typically Microsoft Word, Excel, Scanned Images and PDFs). The site will allow for the meta-tagging for these attachments to support both site internal search and SEO.

5.4.13 The site will allow for the publication of syndicated news feeds, RSS or similar.

5.4.14 The site will have the ability to configure content publishing workflows by organising users into groups and roles, and subsequently assigning them rights (view, edit, publish, and approve) to sections of the website. These workflows and permissions should be assignable on a content type or content section basis.

5.4.14.1 The site will allow for the configuration of email notifications and alerts to support the workflow process, allowing for alternative publish and approval authorities (to cover for absences).

5.4.14.2 The site will have the ability to enter comments while requesting, approving or rejecting changes.

5.4.15 The site will have the ability to set embargo and expiry dates for content.

5.4.16 The site will allow for site administrators to undo actions and edits across the site.

5.4.17 The site's search function must be site-wide and readily filterable. The search will allow for search on keywords and include the use of wildcards. Search results will be ranked in terms of best fit.

5.4.18 The site will allow for the tracking of traffic statistics via Google Analytics (via Google Tag Manager) or similar

5.4.19 The site must comply with NHS Digital security standards and any prevailing CQC and Healthwatch England guidance.

5.4.20 The site will comply with W3C accessibility standards.

5.4.21 The site should work on standard supported web browsers across both desktop and mobile devices.

5.4.22 The site will adhere to Healthwatch England Brand guidelines.

6 Cost Envelope

Please note that any tender responses that exceed the cost envelopes below will be automatically disqualified from the evaluation process.

Lot 1: Hosting and Maintenance (Drupal websites and CiviCRM)	
Lot 2: Support for Drupal based corporate websites, CiviCRM website and CiviCRM local sites	
Lot 3: Development of CiviCRM website and CiviCRM local sites	
Lot 4: Training for CiviCRM Users	
Lot 5: Development of Healthwatch corporate websites	
Total Cost Envelope:	

healthwatch

7 Contractual Arrangements

7.1 Contract Length and Financial Obligations

[redacted]

[redacted]

[redacted]

7.1.1 Time and Material Rates

These rates will apply to any consulting time purchased from the Contractor by the Authority during the duration of the contract (1st October 2019 to 31st March 2021) with the option to extend for a further six to twelve months.

These rates will only apply to pure time and materials work with monthly invoicing based on time worked and payment within 30 days of a correctly prepared invoice.

These prices are exclusive of expenses.

The rate card shall apply for 7.5 hour working days between the hours of 09:00 and 17:30.

All prices are exclusive of VAT.

7.1.2 Payment Schedule

The contractor is required to invoice on a monthly basis upon contract signature.

The Purchase Order provided by the Authority must include the following information:

- A valid and unique Purchase Order reference which will be recognised by the Authority's Accounts Payable Department.
- Delivery contact and address
- Invoice contact and contact number
- Description of products and services to be provided and associated costs (exc. VAT)

7.1.3 Pricing Assumptions

1. The Authority shall pay within 30 days of receipt of a correctly prepared invoice
2. If significant change orders are raised, parties will renegotiate the Payment Schedule
3. Prices are exclusive of VAT
4. Invoice dates of options will be agreed when taken up

7.2 Service Credits

A service credit regime will be applied to ensure that the Contractor meets the contracted service levels. If not, the Authority will have rights to financial remedies (by way of service credits). The intent is to ensure that the Authority has the means to resolve sub-standard performance by the Contractor.

The service levels detailed in Section 4 and the Key Performance Indicators in Section 8 provide the measurement for service overall.

In terms of hosting, the availability of the production infrastructure during Core Hours is subject to service credits if it falls below 99.5% (excluding planned and agreed outages) measured over a quarterly period. The first measurement quarter for service credit purposes will commence once the refreshed infrastructure has been accepted into production by the Authority.

The Contractor will apply a credit on an increasing scale for availability below 99.5%, (excluding planned and agreed outages) to be capped at 10% of the quarterly charge for the Contractor element of the managed services in the event that the availability over the quarter was 90% or below as follows:

Availability of infrastructure in core hours	% of quarterly charge to credit
>99.5%	0%
99.5%	0%
98.5%	0.5%
97.5%	1%
96.5%	1.5%
95.5%	2%
94.5%	2.5%
93.5%	3%
93%	3.5%
92.5%	4%
92%	5%
91.5%	6%
91%	7%
90.5%	8%
90%	10%

In terms of support, if, measured over a 3 month period, the Contractor fails to meet its SLA, the

Contractor shall issue the Authority with a credit note for the lesser of £2000 or 5% of the then current annual charge for CiviCRM and Web support.

In the situation where there are less than 11 incidents (total as opposed to breaching) in a 3 month period, the measurement period shall be extended until 11 incidents have occurred.

7.3 Authorities Responsibilities

The Authority will assume project management responsibility for all works undertaken as part of this contract and will plan and attend regular contract management and service delivery meetings.

The Authority will ensure that throughout the duration of the contract all contracted parties will be subject to agreements that will ensure the necessary levels of support are met.

Where necessary the Authority will also ensure that processes and systems are put into place that promote efficiency and ensure effective delivery of requirements and parity between contracted parties.

The Authority retains responsibility for the roll out of software to its end users. Any delay in rollout will not affect pricing.

The Contractor shall recommend applications, databases, operating system patches or upgrades which the Authority will either approve or reject. If rejected, the Contractor will detail the impact on its ability to deliver the services.

The Authority will own and manage all specifications and approve or reject development subsequent to testing.

7.4 Contractors Responsibilities

The Contractor/s will be responsible for delivering the functional and non-functional requirements as set out in Section 4 and 5 of this document and achieving the required service levels as set out in Section 4.

The Contractor/s will appoint a clear point of contact for project management to ensure smooth delivery of the work programmes; this will include regular attendance at meetings via phone or in person and a commitment to reporting progress and maintaining a clear activity log via a chosen communication channel.

The Contractor will provide monthly statement of accounts.

In addition the Contractor/s will be required to operate the service in accordance with the applicable legislation including:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Copyright Designs and Patents Act 1988
- Health and Safety Act 1998
- Freedom of Information Act 2000
- Race Relations Act 1976 (Amendments 2000/2003)
- Disability Discrimination Act 1995
- Sex Discrimination Act 1975
- Equal Pay Act 1970

- Employment Equality Regulation 2003
- Age Discrimination Act 2006
- Employment Equality Regulations 2006
- General Data Protection Regulation (2018)

8 Key Performance Indicators

Indicator	Measured by	Reference Point or Target	Review Date
Hosting and maintenance - Consistent delivery of expected levels of service level availability as outlined in the requirements	Reported availability levels every two months	99.5%	28 October 2019
Support - Response and resolution to support tickets within agreed timeframes	Report provided to Authority on a monthly basis	100% of support tickets resolved within 48 hours	24 February 2020
CRM Development - Increased take up and activity within the CRM system.	Report provided to Authority on a monthly basis	Growth target of 40% increase in activity	25 May 2020
Training - Measure of training satisfaction (and plotted against increase in CRM activity)	Monthly review of training evaluation feedback	Increase in satisfaction levels of training recipients (baselined against December 2017 data)	02 December 2019
Web development – website equally responsive on both desktop and mobile devices	Measured by Pingdom or analogous web measurement software. User survey also conducted	Target of home page load time of less than 1.5s on both desktop and mobile. User survey to show satisfaction rate of over 60%	28 October 2019

8.1 Milestones

The majority of the requirements set out in this document relate to the ongoing support, hosting and maintenance of existing systems. Performance for Lot 1, Lot 2,Lot 3 and Lot 4 in particular will be measured against the defined service levels and key performance indicators set out above.

Work linked directly to new or ongoing website development projects will be subject to the establishment of agreed milestones upon award of the contract.

healthwatch

9 Exit Management

The contractor is required to ensure the orderly transition of the service from the Contractor to the Authority and/or Replacement Contractor in the event of termination or expiry of contract. This section sets out the principles of the exit and service transfer arrangements that are intended to achieve an orderly transition which shall form the basis of the Exit Plan.

9.1 Contract Obligations

During the term of the contract the Contractor/s will maintain a document that will detail the technical infrastructure. This document should be detailed enough to permit the Authority and/or replacement contractor/s to understand how the Contractor/s provide the service. This will enable the smooth transition with minimal disruption.

Each party will appoint an Exit Manager and provide written notification of such appointment to the other party within 3 months of the effective date. The Contractor's Exit Manager will be responsible for ensuring that the Contractor and its employees, agents and sub-contractors comply with the schedule. The parties' Exit Managers will liaise with one another in relation to all issues relevant to the termination of the contract and all matters connected with this schedule and each party's compliance with it.

The new supplier will be required to continue existing digital discovery works that are underway (see page 9, Lot 3, 2nd bullet point) in which are integral to the continuation of our digital programme and delivery.

9.2 Exit Plan

The Contractor/s will, within three months after the award of the contract, deliver to the Authority an Exit Plan which sets out he Contractors proposed methodology for achieving an orderly transition of Services from the Contractor to the Authority and/or its replacement contractor on the expiry or termination of this contract. The Plan will comply with the requirements set out below.

Within 30 days after the submission of the Exit Plan, the parties will user their respective reasonable endeavours to agree the contents of the Exit Plan.

The Exit Plan should contain as a minimum:

- The management structure to be employed during both the transfer and cessation of the services
- A detailed description of both the transfer and cessation processes, including a timetable.

9.3 Termination Services

During the termination assistance period or such shorter period as the Authority may require, the Contractor will continue to provide the services (as applicable) and will, at the request of the Authority provide the Termination Services. The Contractor will also provide any reasonable assistance to allow the services to continue without interruption following the termination or expiry of the contract and to facilitate the orderly transfer of responsibility for and conduct of the services to the Authority or replacement contractor.

Prior to the commencement of the termination service the parties will agree the costs of providing them. The costs shall be as agreed between parties no less than 3 months prior to the end of the term or within one month of announcement of the contract termination and should underpin the Exit Plan.

During the termination period service levels should remain unaffected.

Schedule 1A – Supplier Response

LOT 1 Hosting and Maintenance Response:

We are one of the UK's leading open source specialist agencies with strong technical and design skills and wide experience of consulting on, implementing, hosting and supporting a range of complex community websites. We have been working with Drupal and CiviCRM since 2006 and currently support well over a hundred clients on this platform, including NGOs and charities, international corporations, Local Infrastructure Organisations, educational institutions, a political party and a UN agency. We believe that the breadth of our experience and depth of our knowledge makes us ideally placed to undertake this project. We are very excited about the possibility of working with HealthWatch and believe we could continue to provide you with an effective, scalable and future-proof CRM that will be easy to maintain.

Regards

[redacted]

1 Overview

The key partners in the business, [redacted], have been working together for more than fifteen years now and most of the other members of the team are experienced professionals who have been in the industry for a similar length of time. We are based in Bristol but have clients all over the UK, Europe and beyond. We aim to develop long term working relationships with our clients, supporting their development and adding new features to their websites and contact databases as they become more sophisticated users of those systems. Our preference is to work with open source software, as this provides cost benefits, better security and faster development times. We feel this is particularly relevant when working with publicly funded organisations where not just value for money is paramount but where the ethos of sharing knowledge is part of the value system. We specialise in building and consulting on complex Drupal and CiviCRM systems and have been regular contributors to both projects but especially CiviCRM with performance optimisations, bug-fixes, core code updates and sponsored features. We have completed over two hundred projects based on this platform to create systems to manage publishing, membership organisations and communities, e-commerce platforms, service delivery monitoring and more: for commercial clients the public and third sectors. We currently provide hosting, support and elements of the development plan for HealthWatch and have been involved in this project since 2013. We think our proven ability to bring to the table our extensive knowledge of these excellent open source products and experience of working with HealthWatch England makes us ideally placed to collaborate on this project. Our knowledge of the Local HealthWatch network gained from early stage interviews and on -site visits gives us insights in their needs and issues that can be extremely valuable when planning and implementing future development. We build websites, intranets, back office systems and complex community portals. We work with high impact organisations across the UK – ranging from small grassroots charities like One25 www.one25.org.uk (a Bristol based charity founded in 1995 as the only organisation specifically supporting street sex-working women), to large scale national operations like The Green Party who have highly customised workflows in their members' CiviCRM database allowing various levels of access, moderation and control to a [redacted]

Why chose Circle for Hosting and Maintenance services?

Circle focus on the hosting and ongoing support of our clients as a key part of our business model as we recognise that the continued high quality operation of systems is crucial to the success of these organisations. We employ 2 specialist systems administrators and have 2 other staff with

strong sysadmin experience on our team as we believe this aspect of our work is crucial and we know that the experience of these members of our team is extremely helpful at various stages of the development cycle and in being able to investigate and solve operational issues that application developers and software engineers sometimes miss. Our hosting environment is an extremely stable one based on Linux, Nginx and Apache with built in redundancy at every level. We run scores of servers optimised for Drupal and CiviCRM in data-centres around the country and our in-house sysadmins monitor these constantly for load and availability. Our servers are located in high-quality data centres and all use RAIDed hard disks for additional resilience. We provide a fully managed service, which includes hosting, semi-automated backups and security upgrades.
We maintain a suite of tools for rapidly deploying changes across our network, following a strict git workflow to ensure all changes are properly tested and signed off.

2 Data Centre Capability & Resilience

2.1 Experience of hosting CiviCRM & Drupal

We have been providing hosting, maintenance and support for Drupal and CiviCRM sites since 2006. We provide full operating system and server management, including security upgrades and daily backups, as well as full maintenance to the application software used. Circle run several dedicated machines on which we offer shared hosting of Drupal, CiviCRM and WordPress - this is a fully managed hosting service, including daily automated backups of data and regular security upgrades to the application software. For some clients, including HealthWatch England, we supply dedicated and/or virtual machines, which allow our clients more control over their hosting and greater scalability. We also provide customised hosting support for independent consultants and small agencies – providing them with a solid hosting service that they resell as their own leaving us to take care of all the systems and application updates, security and even DNS.

2.2 Sizing constraints

There are no actual sizing constraints with Circle hosting since it based on multiple machines with large disks. In the event that further capacity is required, additional hardware can be deployed as needed.

2.3 Where are the sites hosted?

We propose that the HealthWatch CiviCRM and Drupal sites would continue to be hosted on a high performance physical servers provided by Bytemark, which not only offers exceptional levels of performance at a reasonable price, but are also extremely stable and resilient to hardware failures. All this hosting is in the UK and complies with e-commerce level security requirements and GDPR requirements. Bytemark are a subsidiary of Iomart plc. Their data centres have multiple layers of access control and they routinely deal with UK government and health care contracts. Bytemark have ISO 27001 accreditation, are a Crown Commercial Supplier and have been awarded the Fair Tax Mark. More information about their network and data centres can be found at https://www.bytemark.co.uk/company/data-centres/. When the hosting service was set up there was a significant price and performance advantage in the current configuration over pure cloud-based solutions. There continues to be a significant price advantage although cloud offerings do have better resilience and the ability to scale up as needed. It's not clear that there is an advantage in a cloud approach to this hosting given the scale, but as the growth of the uptake in CRM has

slowed, we would recommend looking into rationalising the current three CRM servers into two. We think that the latest offerings in terms of hardware would be able to serve up the current systems with significant spare capacity. We also think there should be a review of the separation of CRM and websites following a more general review of future functionality as there is potential to do more with integration between Drupal and CiviCRM if these share access to a database and this could also lead to future cost savings.

2.4 Network Neutral?

Circle are Network Neutral and have no commercial tie ins with any network provider or vendors. We currently manage hosted Drupal/CiviCRM instances on [redacted], [redacted], [redacted] and [redacted] hosting environments amongst others. Due to the complexity of the HW CRM system, we have previously worked with HealthWatch England to provide the best value physical hosting based on a high quality UK based provider that is ISO 27001 accredited and would continue to do this. We periodically review our hosting options internally and are satisfied that the current provider offer excellent value for money, the highest levels of security and highly responsive customer service.

2.5. Our compliance with the Data Protection Act & GDPR

We regard all data handled by us as confidential and will only use any client's data as part of troubleshooting or development. We are registered with the ICO as a data processor and are committed to complying with the Data Protection Act and GDPR. We will only keep versions of the database that we need for development and backup purposes and will delete all data not needed. All databases are held on highly secure servers which require at least two levels of authentication to access and only allow access over secure (encrypted) connections. We have policies in place to ensure we will never store client data on laptops, USB sticks or other portable devices that could be removed from our office. All our staff are subject to non -disclosure agreement which covers all details of their work but especially data. All our servers are based in the UK and we will never transfer data outside the UK except with the express agreement of the client. All our hosting complies with at least e-commerce level security requirements and Data Protection requirements.

2.6 Backup procedures

Backups take place nightly. We store backups on Amazon S3 based in London and perform tests of the recovery process several times a year. How long the process takes depends mainly on the size of the database and files directories but we aim to be able to restore systems with 24 hours of a catastrophic failure and would expect most systems to be recoverable in less than that. We take incremental back ups of all files and data once a day on the live server and move the most recent backup off site to an Amazon S3 'bucket' located in London. All backup files are encrypted and moved over secure connections.

2.7 Disaster recovery

We are extremely risk-averse and attempt to mitigate all risks with backup and redundant systems. This applies to our hosting environment, daily work and extends to our phone systems. Our servers use mirrored RAID hard disks so even if a disk fails, your site will continue to operate. In reality, we monitor disks quite carefully and have systems in place that warn us when they spot errors at the disk level starting occur as this can be a pre-cursor to total disk failure and allows us to replace disks that are starting to have problems. We also monitor all our own and client servers and receive warnings if services fail or load increases to more than predetermined levels. We take full backups every 10 days so that we never have to go through more than nine days of incremental backups to

restore. This means that in the event of a major disaster occurring resulting in a data-centre no longer being available, we could restore to a version not more than twenty-four hours old.

2.8 Power outages at data centres

Our servers are located in high-quality data centres that have the following mitigating measures in place for power outages:

Bytemark YO26 -

1MVA primary power supply from a dedicated substation on the 11kV distribution ring. Backup generator with 24 hour runtime and a six hour priority fuel supply contract. Uninterruptible Power Supply system delivering power with N+1 resiliency and option of N+N.

3 Security

3.1 Protecting client data

Circle Interactive has ISO 27001 accreditation. As part of this accreditation process we have designed and implemented an Information Security Management System (ISMS) - a set of policies and procedures for systematically managing Circle's sensitive data. The goal of our ISMS is to minimise risk and ensure business continuity by pro-actively limiting the impact of a security breach. We can share the ISMS individual policies with HealthWatch England. Circle deal with sites that handle a wide range of sensitive and confidential data. Security, confidentiality and data-protection are at the heart of our thinking and we maintain strong security procedures around access to all our servers and data. We ensure amongst other things that systems are secure by design, strong passwords are in use by all our users, and all network traffic takes place over SSL. We only use UK hosting with extremely high physical data-centre security and some of our servers are PCI scanned to ensure compliance with e-commerce standards. Secure password protocols are observed and server passwords will adhere to good practice, using industry -standard levels of security (>15 characters and must include all of: upper and lower case a-z, numbers and special characters). Only permanent staff with sysadmin level of trust have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. Additionally we run regular technical briefings in which we ensure that all members of the development team and project managers are kept up to date with OWASP principles and that our development work is undertaken with these principles at its core.

3.2 Security at Data Centres

All Bytemark data centres are based in the UK and complies with e-commerce level security requirements and Data Protection requirements. Their data centres have multiple layers of access control and they routinely deal with UK government and health care contracts. Bytemark have ISO 27001 accreditation, are a Crown Commercial Supplier and have been awarded the Fair Tax Mark.

3.3 Security vetting of staff

We follow the Basic Personnel Security Standard. We confirm ID from a passport or driving license with photo id, obtain references, and keep copies of these on record. If employing anyone who is not British we confirm their right to work through either EU citizenship, or work visa. We have recently brought in basic disclosure checks and are aware of the procedures for checking and recording date/relevant documentation when employing anyone from outside the EU.

3.4 Confidentiality procedures

We regard all data handled by us as confidential and will only use any client's data as part of troubleshooting or development. We will only keep versions of the database that we need for development and backup purposes and will delete all data not needed. All databases are held on highly secure servers which require at least two levels of authentication to access and only allow access over secure (encrypted) connections. We will never store client data on laptops, USB sticks or other portable devices that could be removed from our office. All our staff are subject to non-disclosure and confidentiality agreements which covers all details of their work but especially data. Circle Interactive provide training to all employees to help them understand their responsibilities when handling data. Employees are required to request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection. Circle employees are required to keep all data secure, by taking sensible precautions and we issue the following guidelines:

• Strong passwords must be used and they should never be shared. (>15 characters and must include all of: upper and lower case a-z, numbers and special characters).
• Password managers should be used to enable the use of strong passwords.
• Personal data should never be disclosed to unauthorised people, either within the company or externally.
• The only people able to access data are those who need it for their work.
• Data should not be shared informally.
• When access to confidential information is required, employees are required to request it from their line managers.

Only permanent staff with sysadmin level of trust will have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. These policies apply to all Circle staff including temporary staff, hosted staff, contractor and secondees.

3.5 Access to data controls and potential breaches

Formal procedures are in place to control the allocation of access rights to information systems and services. These procedures cover all stages in the lifecycle of user access (from initial registration of new user accounts to deletion of access rights when user accounts are no longer required). Special attention is given to the allocation and management of privileged user rights but our basic principle is that the only people able to access data are those who need to for their work. We manage access to systems through a periodic review of the Information Security Management Team and this is implemented by the Sysadmin Team. Circle Interactive has in place an incident reporting mechanism that details the procedures for the identifying, reporting and recording of security incidents. Circle continually update and inform Circle staff of the importance of the identification, reporting and action required to address incidents, to ensure they are proactive in addressing these incidents as and when they occur. We foster a culture of proactive incident reporting and logging which we believe will help reduce the number of security incidents that could otherwise go unreported and unnoticed.

4 Service Management

4.1 Managing client engagement

Our relationships with our clients is extremely important to us and we aim to engage with people at various levels in the client organisation from strategic conversations with senior management to daily conversations with end users through support.

4.2. Roles & responsibilities

The dedicated Service Management Team at Circle would typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Sysadmin – server infrastructure
Senior Developer – technical input as required
Support – escalated assistance via ticket/call
Others as necessary

We'd expect the HealthWatch England (HWE) Service Management Team to typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Support – 1st line HWE England support, escalating to Circle
Others as necessary

4.3 Standard service & performance reporting methods/frequencies

We always aim to offer our clients the level of support they need at regular preagreed intervals. The provision of these services will be pre-aligned to HealthWatch England's and their users needs. Services will be delivered to a defined quality, sufficient to satisfy requirements identified from business processes. A clear service portfolio will be developed and maintained as the basis for all service delivery and service management activities. For all services, a corporate level SLA and/or specific SLAs, which have been agreed with relevant stakeholders, will be in place. We will normally provide weekly phone updates on the progress of all development work, tickets and incidents. Resolved/completed issues will be further listed in billing and we maintain an ongoing spreadsheet of all support tickets resolved. This currently lists which tickets were closed during which month. Our internal monitoring also measures time to first response on tickets and numbers of tickets in certain statuses for more than a given time. We'd be happy to explore additional reporting that we can supply to HWE on your tickets.

4.4 Security and audit reporting

Our security procedures cover all stages in the life-cycle of user access, from initial registration of new user accounts to deletion of access rights when user accounts are no longer required and special attention is given to the allocation and management of privileged user rights. The management team review these procedures periodically and audits are performed by external auditors. We can share these policies and procedures and subsequent reports with HealthWatch England. The current HW admin role have access to all user access logs through the UI and we can supply additional details of server access logs if required. This could be incorporated into a monthly status report if required.

4.5 Dedicated Service Management Team

The dedicated Service Management Team at Circle would typically consist of:
Project Director - strategic
Project Manager – day to day management & communications Sysadmin – server infrastructure
Senior Developer – technical input as required
Support – escalated assistance via ticket/call
Others as necessary

We'd expect the HealthWatch England (HWE) Service Management Team to typically consist of:
Project Director - strategic
Project Manager – day to day management & communications
Support - 1st line HWE England, escalating to Circle Others as necessary

4.6 Monitoring and recording of system access for our staff

As part of our ISMS we have a process for granting access to systems for those team members that need it and we run a monthly scan of user accounts which is reviewed so any unnecessary accounts can be closed. A list of your staff users and their access to the systems could be incorporated into a monthly report if required

4.7 Circle Service desk interface with HealthWatch England

1st line: HWE dedicated support, triage and deal with or escalate to Circle
2nd line: HWE support submit ticket to Circle support desk where it is dealt with by either Project Manager or Support team or escalated within Circle 3rd line: Escalate to developer/sysadmin

Performed during normal working hours 9am – 5pm UK time. Out-of-hours support services may be provided by prior arrangement. We will provide HWE with user accounts for our support site to enable the creation and tracking of support tickets through this interface and so you can upload images (such as screen shots) relevant to the issue. We will monitor all tickets created through this system regularly throughout the working day. In the case of some issues where there is an element of particular urgency or a complication that is difficult to describe through a written report, we are available to discuss issues on the phone as well. We would expect this to normally be restricted to HWE staff but acknowledge that in some cases it may be sensible to include Local HW staff at HWE's discretion. For more urgent issues, or when a call may be more efficient to resolve an issue than an exchange on the ticket system, we will sometimes call your staff or take their calls. We'd expect this to be an adjunct to the ticketing system so that information is still recorded there for reference. We respond to all tickets according to the following schedule:

Category	Description	Response Time	Resolution Time	Hours of Cover
Severity 1	Entire system unavailable to all users	15 minutes	4 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 2	Specific modules of system unavailable to all users	30 minutes	8 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 3	Severe functionality defect	1 hour	12 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 4	Minor functionality defect	1 hour	Scheduled outage to resolve	08:00-20:00 Mon-Fri exc Public Holidays

4.8. Incident categorisation and management

As part of the ISO 27001 accreditation process, we have an Incident Management Policy giving clear guidance, policies and procedures and can share this policy with HealthWatch England. Along with this policy, Circle are fostering a culture of proactive incident reporting and logging to help reduce the number of security incidents that could otherwise go unreported and unnoticed. We have monitoring in place that can trigger incident reporting and in cases of this, as well reporting the incident for our internal processes, we'll also notify your team. Circle's responsibilities and response to incidents:

• incidents are reported in a timely manner and are properly investigated
• incidents are handled by appropriately authorised and skilled personnel
• appropriate levels of management are involved in the determination of response actions
• incidents are recorded and documented
• the impact of the incidents are understood and action is taken to prevent further damage
• external bodies or data subjects are informed as required
• the incidents are dealt with in a timely manner and normal operations restored
• the incidents are reviewed to identify improvements in policies and Procedures

5 Exit

During the course of the contract, we would maintain documents that will detail the technical infrastructure, support processes and development work undertaken. Transition may require the production of additional documentation and/or training for the in-coming provider and we'd provide this to whatever extent you determine is necessary as part of the contract. At the point where this contract would be terminated and taken over by another party or taken in-house, following written confirmation of the above, we would appoint a single person to act as the Exit Manager and this would likely be one of the main points of contact during the operation of the contract. The Circle exit manager and the HWE exit manager would between them draw up a plan and timetable for the transfer of documentation, winding down of any services and any interim management structure that may be needed to ensure a smooth transition with minimal disruption. If interim assistance is required during or after the termination of our main services, these would be agreed as part of the plan and timing and cost of these services would form part of the overall exit plan. Our exit manager

would ensure that we would provide full cooperation and effect the transition with minimal disruption. In particular they would liaise with the exit manager from HWE and ensure that all documentation is properly listed and that the transfer of all assets takes place including but not limited to:

- any custom code base
- access to all code repositories
- access to all production servers and test environments
- notes and documentation relating to development
- support tickets
- backups
- any encryption keys and other cryptographic controls
- domains

During the course of our involvement with this project we have also set up contracts on behalf of HealthWatch England such as the contract for several dedicated and virtual servers and we would need to transfer those contracts to HealthWatch England or another party on exit or before this. Following transfer of all assets to their new controller and acceptance of that process, and following final cessation of the services we would then destroy all unnecessary records and data relating to this project, by shredding paper and securely wiping all digital copies ensuring in particular that no personal data remains on our systems. We would of course need to retain some records of work done and financial transactions for our internal reference and these would be kept in accordance with our record retention policy.

6 Cost

To host up to 148 CiviCRM based sites as described will c[redacted]The contract to host the LHW Drupal sites will be held separately with the LHW sites and there will be no additional cost to HWE as long as the number of sites hosted as part of that deal does not drop below 40.

CQC ICTC 806 Lot 2

Lot 2: Support
August 2019

Circle Interactive

Connecting, Supporting, Empowering

Care Quality Commission

Crown Commercial Service Supplier

LOT 2 Support Response:

We are one of the UK's leading open source specialist agencies with strong technical and design skills and wide experience of consulting on, implementing, hosting and supporting a range of complex community websites. We have been working with Drupal and CiviCRM since 2006 and currently support well over a hundred clients on this platform, including NGOs and charities, international corporations, Local Infrastructure Organisations, educational institutions, a political party and a UN agency. We believe that the breadth of our experience and depth of our knowledge makes us ideally placed to undertake this project. We are very excited about the possibility of working with HealthWatch and believe we could continue to provide you with an effective, scalable and future-proof CRM that will be easy to maintain.

[redacted]

[redacted]

1 Overview

The key partners in the business [redacted], have been working together for more than fifteen years now and most of the other members of the team are experienced professionals who have been in the industry for a similar length of time. We are based in Bristol but have clients all over the UK, Europe and beyond. We aim to develop long term working relationships with our clients, supporting their development and adding new features to their websites and contact databases as they become more sophisticated users of those systems.
Our preference is to work with open source software, as this provides cost benefits, better security and faster development times. We feel this is particularly relevant when working with publicly funded organisations where not just value for money is paramount but where the ethos of sharing knowledge is part of the value system. We specialise in building and consulting on complex Drupal and CiviCRM systems and have been regular contributors to both projects but especially CiviCRM with performance optimisations, bug-fixes, core code updates and sponsored features. We have completed over two hundred projects based on this platform to create systems to manage publishing, membership organisations and communities, e-commerce platforms, service delivery monitoring and more: for commercial clients the public and third sectors. We currently provide hosting, support and elements of the development plan for HealthWatch and have been involved in this project since 2013. We think our proven ability to bring to the table our extensive knowledge of these excellent open source products and experience of working with HealthWatch England makes us ideally placed to collaborate on this project. Our knowledge of the Local HealthWatch network gained from early stage interviews and on-site visits gives us insights in their needs and issues that can be extremely valuable when planning and implementing future development. We build websites, intranets, back office systems and complex community portals. We work with high impact organisations across the UK – r[redacted] you [redacted]

Your patience, counsel, advice and support has always been of tremendous value and I don't think we would have made anywhere near the progress we have done without your help.

Why chose Circle for Website and CRM Support services?

Circle focus on the hosting and ongoing support of our clients as a key part of our business model as we recognise that the continued high quality operation of systems is crucial to the success of these organisations. We employ 2 specialist systems administrators and have 2 dedicated support staff on our team as we believe this aspect of our work is crucial and we know that the experience of these members of our team is extremely helpful at various stages of the development cycle and in being able to investigate and solve operational issues that may occur from time to time.

Any support issues not easily dealt with by this team will be escalated to the development team: 8 experienced developers, many of whom have spent in excess of 10 years working on Drupal and CiviCRM and 3 of whom have long term involvement with the CiviCRM core team. Our support team along with all our staff, use a platform that we've developed based on Drupal and CiviCRM – the applications we're supporting so all our team are fully aware of all aspects of the system from their own day to day experience. We maintain a suite of tools for rapidly deploying changes across our network, following a strict git workflow to ensure all changes are properly tested and signed off.

2 Support

2.1 Experience of providing support for CiviCRM & Drupal

We have been providing hosting, maintenance and support for Drupal and CiviCRM sites since 2006. Circle support clients in their use and maintenance of CiviCRM, Drupal and WordPress using our support ticket system built in Drupal and CiviCRM and adapted specifically for the type of support we offer with notifications of new tickets, time recording and issue categorisation. We currently provide hosting, support and elements of the development plan for HealthWatch and have been involved in this project since 2013. We think our proven ability to bring to the table our extensive knowledge of these excellent open source products and experience of working with HealthWatch England makes us ideally placed to collaborate on this project. Our knowledge of the Local HealthWatch network gained from early stage interviews and on-site visits gives us insights in their needs and issues that can be extremely valuable when planning and implementing future development.

2.2 How we handle support enquiries

Our Help Desk supports hundreds of users from over one hundred organisations as well as the HealthWatch account which covers over 100 instances. All support is delivered and monitored using our in-house Ticketed Support System which is also built on a framework of Drupal & CiviCRM so even our least technical administrators are familiar with these 2 platforms. We also provide telephone support during office hours. HealthWatch have a dedicated Account/Project Manager who is automatically subscribed to any ticket submitted by anyone in HeathWatch England who has the permissions necessary to access to do so. Support issues are initially raised from the LHW network to HWE and when HWE staff are unable to deal with the issues, the Circle Help Desk acts as second line for:

- Diagnosing issues
- Providing "how to" guidance
- Restoring from backups
- Fixing things users have got slightly wrong
- Monitoring roll-out of new instances
- Minor change requests from LHW

Internally we operate a tiered response with simple issues being dealt with by our first line support team, then escalated to sysadmin or developer resources as appropriate to the nature of the ticket. As a ticket is re-assigned or escalated to another member of staff, they can see the full conversation that has taken place to date. Your users can create and track support tickets through this interface and upload images (such as screen shots) relevant to the issue across 4 main sites. We monitor all tickets created through the support system regularly throughout the working day.

We guarantee to respond to all tickets (submitted via support) according to the following schedule:

Category	Description	Response Time	Resolution Time	Hours of Cover
Severity 1	Entire system unavailable to all users	15 minutes	4 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 2	Specific modules of system unavailable to all users	30 minutes	8 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 3	Severe functionality defect	1 hour	12 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 4	Minor functionality defect	1 hour	Scheduled outage to resolve	08:00-20:00 Mon-Fri exc Public Holidays

We categorise support tickets as:
- Change Request
- Snagging (following project work)
- Investigation of perceived issues
- Training issue – user hasn't understood how to do something
- Restore from backup
- Bug report in underlying software
- Security incident

We review tickets quarterly across our whole operation to monitor trends. We then communicate with clients who seem to have e.g. a growing number of training issues in order to suggest training options for them. We will send you a quarterly overview of the type of support issues that are coming through to help HWE either communicate better with the network or provide specific training to deal with these issues.

2.3 Project Management & forward planning

As part of our support work we expect to be involved in planning of development work undertaken by our team or other partners and working with the HWE team and other partners to facilitate this. Our preferred methodology for all development is to always take an Agile approach and we hold periodic workshops for the whole development team to ensure our own agile framework constantly improves. Our framework allows for flexibility and focusses on the practical consequences of any work as it will affect the delivery of the finished product. Our methodology involves aspects of Scrum and XP but adapted to suit the nature of the type of projects we typically work on. We plan sprints of a suitable time for the chunk of work being undertaken – typically 2 to 3 weeks. We will always have a working piece of software at the end of that sprint for review though not all elements may be complete. We often work in XP style pairs with two pairs of eyes on the code to ensure quality and aid us in security planning. We think the most important step in any major database change is the

planning phase. Without effective, strategic planning aligned to organisational goals, a project will often go ‘off the rails’ and end up exceeding both the expected time limit and budget. It's also important to have sufficient technical planning to ensure a range of issues are considered including dependencies technical constraints and uncertainties. At Circle, we like to take our clients through an extensive ‘discovery’ process, where we gather as much relevant information about the proposed workflows and anticipated benefits as we can. We then have a clear sense of the project and its benefits, including how our developers can work best alongside a client’s existing team to ensure a smooth transition to the new system.

3 Security

3.1 Protecting client data

Circle Interactive has ISO 27001 accreditation. As part of this accreditation process we have designed and implemented an Information Security Management System (ISMS) - a set of policies and procedures for systematically managing Circle's sensitive data. The goal of our ISMS is to minimise risk and ensure business continuity by pro-actively limiting the impact of a security breach. We can share the ISMS individual policies with HealthWatch England. Circle deal with sites that handle a wide range of sensitive and confidential data. Security, confidentiality and data-protection are at the heart of our thinking and we maintain strong security procedures around access to all our servers and data. We ensure amongst other things that systems are secure by design, strong passwords are in use by all our users, and all network traffic takes place over SSL. We only use UK hosting with extremely high physical data-centre security and some of our servers are PCI scanned to ensure compliance with e-commerce standards. Secure password protocols are observed and server passwords will adhere to good practice, using industry -standard levels of security (>15 characters and must include all of: upper and lower case a-z, numbers and special characters). Only permanent staff with sysadmin level of trust have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. Additionally we run regular technical briefings in which we ensure that all members of the development team and project managers are kept up to date with OWASP principles and that our development work is undertaken with these principles at its core.

3.2 Security vetting of staff

We follow the Basic Personnel Security Standard. We confirm ID from a passport or driving license with photo id, obtain references, and keep copies of these on record. If employing anyone who is not British we confirm their right to work through either EU citizenship, or work visa. We have recently brought in basic disclosure checks and are aware of the procedures for checking and recording date/relevant documentation when employing anyone from outside the EU.

3.3 Confidentiality procedures

We regard all data handled by us as confidential and will only use any client's data as part of troubleshooting or development. We will only keep versions of the database that we need for development and backup purposes and will delete all data not needed. All databases are held on highly secure servers which require at least two levels of authentication to access and only allow access over secure (encrypted) connections. We will never store client data on laptops, USB sticks or other portable devices that could be removed from our office. All our staff are subject to non-disclosure and confidentiality agreements which covers all details of their work but especially data. Circle Interactive provide training to all employees to help them understand their responsibilities when handling data. Employees are required to request help from their line manager or the Data

Protection Officer if they are unsure about any aspect of data protection. Circle employees are required to keep all data secure, by taking sensible precautions and we issue the following guidelines:
• Strong passwords must be used and they should never be shared. (>15 characters and must include all of: upper and lower case a-z, numbers and special characters).
• Password managers should be used to enable the use of strong passwords.
• Personal data should never be disclosed to unauthorised people, either within the company or externally.
• The only people able to access data are those who need it for their work.
• Data should not be shared informally.
• When access to confidential information is required, employees are required to request it from their line managers.

Only permanent staff with sysadmin level of trust will have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. These policies apply to all Circle staff including temporary staff, hosted staff, contractor and secondees.

3.4 Access to data controls and potential breaches

Formal procedures are in place to control the allocation of access rights to information systems and services. These procedures cover all stages in the lifecycle of user access (from initial registration of new user accounts to deletion of access rights when user accounts are no longer required). Special attention is given to the allocation and management of privileged user rights but our basic principle is that the only people able to access data are those who need to for their work. We manage access to systems through a periodic review of the Information Security Management Team and this is implemented by the Sysadmin Team. Circle Interactive has in place an incident reporting mechanism that details the procedures for the identifying, reporting and recording of security incidents. Circle continually update and inform Circle staff of the importance of the identification, reporting and action required to address incidents, to ensure they are proactive in addressing these incidents as and when they occur. We foster a culture of proactive incident reporting and logging which we believe will help reduce the number of security incidents that could otherwise go unreported and unnoticed.

4 Development

4.1 Experience of providing development capability for CiviCRM and Drupal

Circle Interactive is proud to have been an active member of both the CiviCRM and Drupal communities for many years. We also have the largest CiviCRM development team based in the UK. As such, we've worked on development projects in collaboration with the Core Team and most of the UK based partners either as lead developers or providing additional capacity to other projects. We've also collaborated internationally with other partners to develop functionality which is only partly funded by client projects. A good example is the integration with [redacted]. We subsequently had a client whose requirements went beyond this and added new features to their early work, before they then found further funding to make some elements more configurable through the UI. In a similar fashion. We've written, co-written and extended several other key financial extensions, in some cases adding reliability to functionality that just can't fail. Some of these are listed below.

4.2 Delivery of new functionality in CiviCRM

CiviCRM Extension granting access for event creators to view their events' participants.
https://github.com/circleinteractive/org.civicrm.vieweventparticipants

Some other examples of our experience of developing features using CiviCRM with a mix of unpublished extensions:
“Lead heat” for an education provider where contacts have different touch points throughout the site and different actions push contact data into CRM creating or adding to a lead score which then produces 'cool', 'warm' and 'hot' leads in the CRM allowing staff to prioritise follow up actions.

Application and processing system for grant giving charity in which people apply for grants within a time-restricted window, the applications are reviewed and assigned to 3 assessors whose judgements are combined to decide whether the applicant should progress to the next stage. In the next stage more information is elicited and applicants have the opportunity to update some details recorded in CiviCRM.

Appraisal tracking system for a medical body in which members need to be annually appraised as part of their professional accreditation. The appraisals happen throughout the year but need to be progressed according to a given schedule. With appraisers, appraisees and administrators all involved, a system of alerts and views of any activity that is behind schedule were needed to keep things moving.

4.3 Delivery of new functionality in Drupal

Some examples of our experience of developing features using Drupal:

Organisation manager – allows an organisation's designated manager to update new staff, remove ex-staff and allocated permissions to the existing staff list. This uses Organic Groups and CiviCRM and is designed for organisations whose members or partner organisations will have multiple users logging in to and interacting with the site at different permission levels.

Support – this has extended the support module to allow for multiple members of a client team to interact on support tickets while allowing support team members to exchange private notes and change the status of the ticket from the comment form.

Quote manager – allows users to submit their details to an insurer who can then issue quotes that the users have to sign accept before going through to pay. The insurer then issues a certificate with the details through the system.

Grant application manager – allows users to save drafts of their application form while building up all the evidence needed to submit. Then puts the application into a holding state while it is assigned to several assessors who score it. Applications with sufficient scores are then moved on to the next round and the original applicant is asked for further details before a more in-depth assessment is made.

4.4 Circle’s approach to development & the wider community

We are active members of the community, providing financial and time inputs, sponsoring events and sending several people to sprints in the UK every year. We contribute code and testing time, collaborate on the development of extensions, writing some ourselves, adding to and improving on others. We also contribute code and testing time to most releases of the product and are actively involved as part of the security team. We provide resources to help with managing the issue queue reviewing Pull Requests from other members of the community. This allows us to stay up to date, helps introduce fixes and gives us credit for when we need to get our own contributions accepted. We also provide support on the main forums (Mattermost and StackExchange) and with community infrastructure (we manage the monitoring of civicrm.org and other resources with nagios and munin).

4.5 Development of applications using Agile methodologies

Our preferred methodology for application development is to always take an Agile approach and we hold periodic workshops for the whole development team to ensure our approach constantly improves. Our framework allows for flexibility and focusses on the practical consequences of any work as it will affect the delivery of the finished product. Working in an agile way does sometimes require a cultural shift in some client organisations because it focuses on the clean delivery of individual pieces or parts of the software and not on the entire application. It also guarantees cost, delivery time, and quality but not outcomes. Our methodology involves aspects of Scrum and XP but adapted to suit the nature of the type of projects we typically work on. We plan sprints of a suitable time for the chunk of work being undertaken – typically 2 to 3 weeks. We will always have a working piece of software at the end of that sprint for review though not all elements may be complete. We often work in XP style pairs with two pairs of eyes on the code to ensure quality and aid us in security planning. We do daily stand-ups though we don't religiously document the backlog on smaller projects where this would add unduly to the admin overhead. We use MoSCoW prioritisation and time boxing to ensure the key features are delivered according to the plan.

Planning Phase (Facilitated Workshops)

We think the most important step in any major database change is the planning phase. Without effective, strategic planning aligned to organisational goals, a project will often go ‘off the rails’ and end up exceeding both the expected time limit and budget. At Circle, we like to take our clients through an extensive ‘discovery’ process, where we gather as much relevant information about the proposed workflows and anticipated benefits as we can. We then have a clear sense of the project and its benefits, including how our developers can work best alongside a client’s existing team to ensure a smooth transition to the new system.

4.6 Experience of integrating CiviCRM with other applications

As described throughout this proposal, we have been working with Drupal and CiviCRM since 2006 and currently support well over a hundred clients on this platform. We have provided integration through API to a range of other applications

communication technology (ICT) more effectively. They appointed Circle Interactive to be their technical partner. The initial specification from SCIE was vague but enough of the outcomes were defined to enable us to decide that CiviCRM and in particular CiviCase would be an appropriate platform. We went through a process of defining the specification more clearly but started work on the assumption that we would be building a prototype to be altered as users from the various organizations started using it. We needed the new system to have a single login and synchronise data both ways with the existing my.scie.org.uk site – a bespoke system written in classic ASP and this required substantial coordination with SCIE's technical team.

4.7 Experience of integrating Drupal with other applications

This is one of our areas of particular expertise and over the years we have built dozens of integrated systems apart from the >100 CiviCRM integrations which range in complexity from simple to extremely complex. In particular we've integrated data and access levels with:

Moodle: We've undertaken several integrations with this online virtual learning environment. These have been mostly single sign ons allowing users to access the Moodle once logged on to the Drupal site where their profile would be stored along with any blogs and forum posts.

SCRAN: www.scran.ac.uk We integrated a community site with this existing platform for a project by Dyslexia Action in conjunction with RNIB. Users logged into the SCRAN system and were able to see some details from their Drupal presence while clicking through in a SSO environment to update those details and take part in discussions on the Drupal.

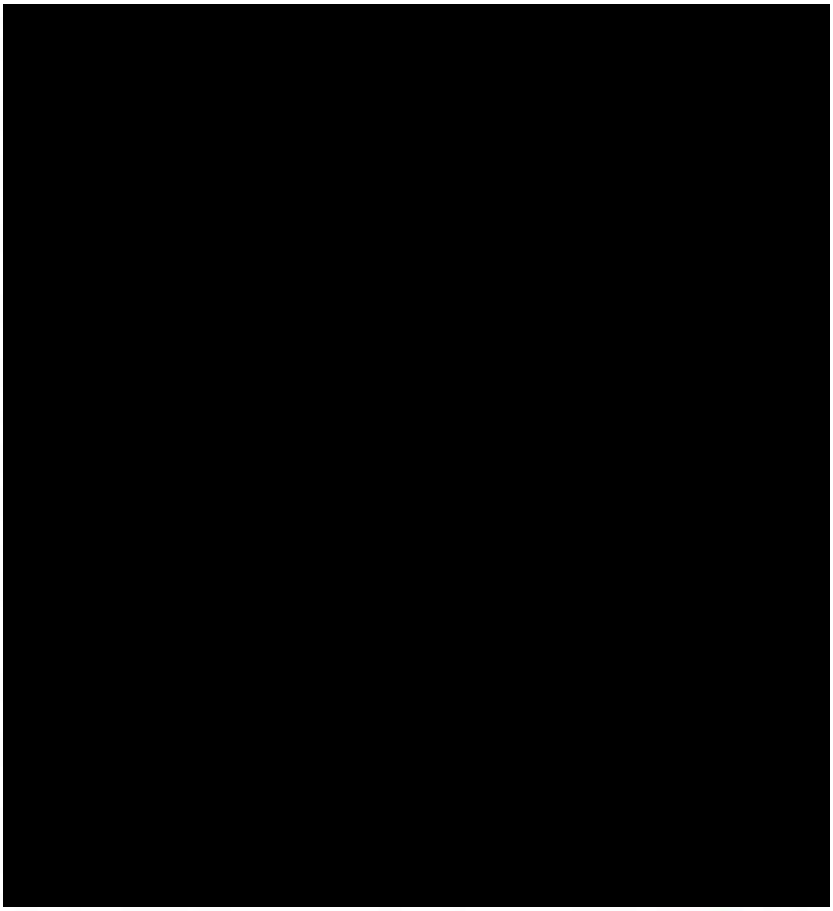
TT Exchange: We've integrated the https://www.tt-exchange.org/ Drupal with a custom application built around CiviCRM by TechSoup which monitors various licencing agreements they have with large vendors such as Microsoft.

SCIE: We built a system that integrated with SCIE's proprietary CMS to allow data syncing across various fields as users applied for grants through a series of Drupal forms, had their profiles listed from SCIE and updated while their application took place through a mix of CiviCRM's Case management and customised Drupal webforms.

4.8 Development of CiviCRM with external suppliers and internal staff

There are advantages of working with multiple teams as they potentially bring different perspectives to the table and can act as controls on each other if all are engaged in planning development work. It's important for all to agree on ways of working and follow processes. We have established a productive working relationship with [redacted] on this project, and we have each strengthened the other's working processes. We've agreed on a successful Git workflow for managing code and this has forced both sets of developers to follow processes that perhaps would have otherwise been easy to shortcut. However, by following the procedures, we've subsequently been able to help fix issues that have come about from the development process.
The git repository will contain the Drupal /sites directory in its entirety. Above this level there are symlinks which would make the repo confusing. We are following this Git Workflow as described in

https://docs.google.com/document/d/1UlcPH3ZdTTPFt9IC5vigZ7swC1f-TxuQRcyEugVqrE/edit



Developer environments
There can be as many dev branches as developers need but they get merged back into a Workstream branch and then into staging so features can be tested before going live.

We maintain a Hot Fix branch which is temporary while security updates are being tested and applied. After Master has security updates merged from Hot Fix, Staging should have that code merged into it from Master by Circle sysadmins and any current Workstream/Feature branches should have that code merged into them. That should be responsibility of the developer(s) using those branches but sysadmins can help with this process if more convenient.

Common communication platform
We normally use our Drupal based intranet as a communications platform between ourselves and clients since we record technical details here and time spent is gathered on this platform. However, when working with multiple parties as on HealthWatch, we are open to using other paltforms such as Basecamp or Jira as a communications platform. We also make use of Google docs for drawing up shared specifications and lists when it helps for multiple people to collaboratively work on something together in real time. It is important to ensure these are archived properly and kept private. In addition we use Smartsheets for project plans, resource planning and dependencies.

8. Our approach to testing and quality assurance

Our developers initially perform functional tests of their work against documentation on their dev environment. When developing CiviCRM extensions or Drupal modules we will use a combination of unit tests if applicable, functional tests as described in the documentation and will often produce Selenium tests to prevent regressions being introduced in future releases.

We involve our support team in testing and documentation of functionality so that they are better able to support the software, but we rely on various members of the team to be involved in this crucial aspect of work, especially other developers and project managers.

5 Service Management

5.1 Managing client engagement

Our relationships with our clients is extremely important to us and we aim to engage with people at various levels in the client organisation from strategic conversations with senior management to daily conversations with end users through support.

5.2 Roles & responsibilities

The dedicated Service Management Team at Circle would typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Sysadmin – server infrastructure
Senior Developer – technical input as required
Support – escalated assistance via ticket/call
Others as necessary

We'd expect the HealthWatch England (HWE) Service Management Team to typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Support – 1st line HWE England support, escalating to Circle
Others as necessary

5.3 Standard service & performance reporting methods/frequencies

We always aim to offer our clients the level of support they need at regular preagreed intervals. The provision of these services will be pre-aligned to HealthWatch England's and their users needs. Services will be delivered to a defined quality, sufficient to satisfy requirements identified from business processes. A clear service portfolio will be developed and maintained as the basis for all service delivery and service management activities. For all services, a corporate level SLA and/or specific SLAs, which have been agreed with relevant stakeholders, will be in place. We will normally provide weekly phone updates on the progress of all development work, tickets and incidents. Resolved/completed issues will be further listed in billing and we maintain an ongoing spreadsheet of all support tickets resolved. This currently lists which tickets were closed during which month. Our internal monitoring also measures time to first response on tickets and numbers of tickets in certain statuses for more than a given time. We'd be happy to explore additional reporting that we can supply to HWE on your tickets.

5.4 Security and audit reporting

Our security procedures cover all stages in the life-cycle of user access, from initial registration of new user accounts to deletion of access rights when user accounts are no longer required and special attention is given to the allocation and management of privileged user rights. The management team review these procedures periodically and audits are performed by external auditors. We can share these policies and procedures and subsequent reports with HealthWatch England.

5.5 Dedicated Service Management Team

The dedicated Service Management Team at Circle would typically consist of:
Project Director - strategic
Project Manager – day to day management & communications Sysadmin – server infrastructure
Senior Developer – technical input as required
Support – escalated assistance via ticket/call
Others as necessary

We'd expect the HealthWatch England (HWE) Service Management Team to typically consist of:
Project Director - strategic
Project Manager – day to day management & communications
Support - 1st line HWE England, escalating to Circle Others
as necessary

5.6 Monitoring and recording of system access for our staff

As part of our ISMS we have a process for granting access to systems for those team members that need it and we run a monthly scan of user accounts which is reviewed so any unnecessary accounts can be closed.

5.7 Circle Service desk interface with HealthWatch England

1st line: HWE dedicated support, triage and deal with or escalate to Circle
2nd line: HWE support submit ticket to Circle support desk where it is dealt with by either Project Manager or Support team or escalated within Circle 3rd line: Escalate to developer/sysadmin

Performed during normal working hours 9am – 5pm UK time. Out-of-hours support services may be provided by prior arrangement. We will provide HWE with user accounts for our support site to enable the creation and tracking of support tickets through this interface and so you can upload images (such as screen shots) relevant to the issue. We will monitor all tickets created through this system regularly throughout the working day. In the case of some issues where there is an element of particular urgency or a complication that is difficult to describe through a written report, we are available to discuss issues on the phone as well. We would expect this to normally be restricted to HWE staff but acknowledge that in some cases it may be sensible to include Local HW staff at HWE's discretion. For more urgent issues, or when a call may be more efficient to resolve an issue than an exchange on the ticket system, we will sometimes call your staff or take take their calls. We'd expect this to be an adjunct to the ticketing system so that information is still recorded there for reference. We respond to all tickets according to the following schedule:

Category	Description	Response Time	Resolution Time	Hours of Cover
Severity 1	Entire system unavailable to all users	15 minutes	4 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 2	Specific modules of system unavailable to all users	30 minutes	8 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 3	Severe functionality defect	1 hour	12 Hours	08:00-20:00 Mon-Fri exc Public Holidays
Severity 4	Minor functionality defect	1 hour	Scheduled outage to resolve	08:00-20:00 Mon-Fri exc Public Holidays

5.8 Incident categorisation and management

As part of the ISO 27001 accreditation process, we have an Incident Management Policy giving clear guidance, policies and procedures and can share this policy with HealthWatch England. Along with this policy, Circle are fostering a culture of proactive incident reporting and logging to help reduce the number of security incidents that could otherwise go unreported and unnoticed. We have monitoring in place that can trigger incident reporting and in cases of this, as well reporting the incident for our internal processes, we'll also notify your team. Circle's responsibilities and response to incidents:

- incidents are reported in a timely manner and are properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of management are involved in the determination of response actions
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and Procedures

6 Exit

During the course of the contract, we would maintain documents that will detail the technical infrastructure, support processes and development work undertaken. Transition may require the production of additional documentation and/or training for the in-coming provider and we'd provide this to whatever extent you determine is necessary as part of the contract. At the point where this contract would be terminated and taken over by another party or taken in-house, following written confirmation of the above, we would appoint a single person to act as the Exit Manager and this would likely be one of the main points of contact during the operation of the contract. The Circle exit manager and the HWE exit manager would between them draw up a plan and timetable for the transfer of documentation, winding down of any services and any interim management structure that may be needed to ensure a smooth transition with minimal disruption. If interim assistance is required during or after the termination of our main services, these would be agreed as part of the

plan and timing and cost of these services would form part of the overall exit plan. Our exit manager would ensure that we would provide full cooperation and effect the transition with minimal disruption. In particular they would liaise with the exit manager from HWE and ensure that all documentation is properly listed and that the transfer of all assets takes place including but not limited to:

- any custom code base
- access to all code repositories
- access to all production servers and test environments
- notes and documentation relating to development
- support tickets
- backups
- any encryption keys and other cryptographic controls
- domains

During the course of our involvement with this project we have also set up contracts on behalf of HealthWatch England such as the contract for several dedicated and virtual servers and we would need to transfer those contracts to HealthWatch England or another party on exit or before this. Following transfer of all assets to their new controller and acceptance of that process, and following final cessation of the services we would then destroy all unnecessary records and data relating to this project, by shredding paper and securely wiping all digital copies ensuring in particular that no personal data remains on our systems. We would of course need to retain some records of work done and financial transactions for our internal reference and these would be kept in accordance with our record retention policy.

7 Cost

The cost of providing 4 days per month of support as detailed here plu [redacted]CiviCRM and Web consultancy will be charged at our standard support [redacted]

CQC ICTC 806 Lot 3

Lot 3: Development (CRM)
August 2019

Circle Interactive

Connecting, Supporting, Empowering

CareQuality Commission

CivicRM Lot 1 Technical Envelope - Classification: Client Confidential

Crown Commercial Service Supplier

LOT 3 Development Response:

We are one of the UK's leading open source specialist agencies with strong technical and design skills and wide experience of consulting on, implementing, hosting and supporting a range of complex community websites. We have been working with Drupal and CiviCRM since 2006 and currently support well over a hundred clients on this platform, including NGOs and charities, international corporations, Local Infrastructure Organisations, educational institutions, a political party and a UN agency. We believe that the breadth of our experience and depth of our knowledge makes us ideally placed to undertake this project. We are very excited about the possibility of working with HealthWatch and believe we could continue to provide you with an effective, scalable and future-proof CRM that will be easy to maintain.

[redacted]

1 Overview

The key partners in the business, [redacted] have been working together for more than fifteen years now and most of the other members of the team are experienced

professionals who have been in the industry for a similar length of time. We are based in Bristol but have clients all over the UK, Europe and beyond. We aim to develop long term working relationships with our clients, supporting their development and adding new features to their websites and contact databases as they become more sophisticated users of those systems.
Our preference is to work with open source software, as this provides cost benefits, better security and faster development times. We feel this is particularly relevant when working with publicly funded organisations where not just value for money is paramount but where the ethos of sharing knowledge is part of the value system. We specialise in building and consulting on complex Drupal and CiviCRM systems and have been regular contributors to both projects but especially CiviCRM with performance optimisations, bug-fixes, core code updates and sponsored features. We have completed over two hundred projects based on this platform to create systems to manage publishing, membership organisations and communities, e-commerce platforms, service delivery monitoring and more: for commercial clients the public and third sectors. We currently provide hosting, support and elements of the development plan for HealthWatch and have been involved in this project since 2013. We think our proven ability to bring to the table our extensive knowledge of these excellent open source products and experience of working with HealthWatch England makes us ideally placed to collaborate on this project. Our knowledge of the Local HealthWatch network gained from early stage interviews and on-site visits gives us insights in their needs and issues that can be extremely valuable when planning and implementing future development.
We build websites, intranets, back office systems and complex community portals. We work with high impact organisations across the UK – ranging from small [redacted]

It's been an immense pleasure to work with you over the past few years and frankly I believe you have been instrumental in the amazing success that we've achieved over that time. Your patience, counsel, advice and support has always been of tremendous value and I don't think we would have made anywhere near the progress we have done without your help.

Projections for company growth

Circle is a stable company established in 2005 that has grown steadily in that time mainly through our reputation as leaders in expertise with CiviCRM. Last year we turned over about [redacted] with a profit of [redacted]. This year we expect that to increase to around £1m with a slightly increased margin. We've built up a client base of over 150 organisations including a political party, several well know large charities, many smaller ones plus a range of private businesses and public sector organisations. We have the largest team of experienced CiviCRM developers based in the UK and are looking to continue our recent growth of between [redacted] Core to this growth are three strands of our business:

- development of new functionality that we share between groups of sites,
- a stable and highly secure hosting environment based in the UK,
- a responsive technical support desk.

As well as providing these services to our clients directly, we also support several independent Drupal / CiviCRM consultants with our hosting and support and sometimes technical elements of development work that they feel we can undertake more effectively than they can. Part of our strategy is to continue to expand these relationships, working collaboratively with others in both Drupal and CiviCRM communities. Our growth plans also include the provision and maintenance of product-like software distributions for certain vertical markets allowing us to build on expertise with e.g. medical associations to provide a platform that several organisations can use and develop with benefits going to all. This is something we've been building gradually over the last few years and which is expanding as a percentage of our turnover. Key to our ability to scale up from this position is reviewing our processes and for several months now we've been undergoing a major initiative to document and review all processes, improving those where there is scope to increase efficiency by having further cross-team involvement.

2 Development

2.1 Experience of providing development capability for CiviCRM

Circle Interactive is proud to have been an active member of both the CiviCRM and Drupal communities for many years. We also have the largest CiviCRM development team based in the UK. As such, we've worked on development projects in collaboration with the Core Team and most of the UK based partners either as lead developers or providing additional capacity to other projects. We've also collaborated internationally with other partners to develop functionality which is only partly funded by client projects. A good example is the integration with Accounting software Xero as this typical of the way much work gets done within the community. Initially New Zealand partner Fusion wrote a basic integration. We subsequently had a client whose requirements went beyond this and added new features to their early work, before they then found further funding to make some elements more configurable through the UI. In a similar fashion. We've written, co-written and extended several other key financial extensions, in some cases adding reliability to functionality that just can't fail. Some of these are listed below.

2.2 Delivery of new functionality in CiviCRM

CiviCRM Extension granting access for event creators to view their events' participants.

https://github.com/circleinteractive/org.civicrm.vieweventparticipants

Some other examples of our experience of developing features using CiviCRM with a mix of unpublished extensions:

“Lead heat” for an education provider where contacts have different touch points throughout the site and different actions push contact data into CRM creating or adding to a lead score which then produces 'cool', 'warm' and 'hot' leads in the CRM allowing staff to prioritise follow up actions.

Application and processing system for grant giving charity in which people apply for grants within a time-restricted window, the applications are reviewed and assigned to 3 assessors whose judgements are combined to decide whether the applicant should progress to the next stage. In the next stage more information is elicited and applicants have the opportunity to update some details recorded in CiviCRM.

Appraisal tracking system for a medical body in which members need to be annually appraised as part of their professional accreditation. The appraisals happen throughout the year but need to be progressed according to a given schedule. With appraisers, appraisees and administrators all involved, a system of alerts and views of any activity that is behind schedule were needed to keep things moving.

2.3. Development of multiple CiviCRM instances:

Greater Manchester Centre for Voluntary Organisations (GMCVO) provide collaborative leadership, communications & co-ordination across Greater Manchester along with some direct services. provide support, knowledge, voice, infrastructure and innovation. Circle created infrastructure for 15 linked instances, initially as a single instance and subsequently as separate instances with common reporting. Documentation for this project was built up on our intranet. Source code is in our private repository.

[redacted]is a charity that supports communities in need, working with partners to help improve the quality of peoples lives and the places where they live, work and play.

[redacted]

HealthWatch England, the national body for the local HealthWatch network consisting of approximately 95 instances. Circle currently provides hosting, maintenance and support to HealthWatch England and the local HealthWatch network with their CRM systems and sites (consisting of >90 instances at this moment in time.) Over the past years Circle have played an instrumental role in the development of the CiviCRM and the fulfilment of the desire for uniform capture of information/data across the cluster. Documentation for this project was built up on our intranet. The source code is held in a private git repository.

CiviSites is a product of Circle Interactive – it is a web-based CRM Software as a Service (SaaS) platform providing an automated low cost standardised distribution for charities that has been taken up by several dozen small charities.
https://www.civisites.com/

Documentation is held on our intranet and in a series of further documents on the server including instructions for build in Docker containers. The source code is held in a private git repository.

2.4 Circle's approach to development & the wider community

We are active members of the community, providing financial and time inputs, sponsoring events and sending several people to sprints in the UK every year. We contribute code and testing time, collaborate on the development of extensions, writing some ourselves, adding to and improving on others. We also contribute code and testing time to most releases of the product and are actively

involved as part of the security team. We provide resources to help with managing the issue queue reviewing Pull Requests from other members of the community. This allows us to stay up to date, helps introduce fixes and gives us credit for when we need to get our own contributions accepted. We also provide support on the main forums (Mattermost and StackExchange) and with community infrastructure (we manage the monitoring of civicrm.org and other resources with nagios and munin).

2.5 Development of applications using Agile methodologies

Our preferred methodology for application development is to always take an Agile approach and we hold periodic workshops for the whole development team to ensure our approach constantly improves. Our framework allows for flexibility and focusses on the practical consequences of any work as it will affect the delivery of the finished product. Working in an agile way does sometimes require a cultural shift in some client organisations because it focuses on the clean delivery of individual pieces or parts of the software and not on the entire application. It also guarantees cost, delivery time, and quality but not outcomes. Our methodology involves aspects of Scrum and XP but adapted to suit the nature of the type of projects we typically work on. We plan sprints of a suitable time for the chunk of work being undertaken – typically 2 to 3 weeks. We will always have a working piece of software at the end of that sprint for review though not all elements may be complete. We often work in XP style pairs with two pairs of eyes on the code to ensure quality and aid us in security planning. We do daily stand-ups though we don't religiously document the backlog on smaller projects where this would add unduly to the admin overhead. We use MoSCoW prioritisation and time boxing to ensure the key features are delivered according to the plan.

Planning Phase (Facilitated Workshops)

We think the most important step in any major database change is the planning phase. Without effective, strategic planning aligned t o organisational goals, a project will often go ‘off the rails’ and end up exceeding both the expected time limit and budget. At Circle, we like to take our clients through an extensive ‘discovery’ process, where we gather as much relevant information about the proposed workflows and anticipated benefits as we can. We then have a clear sense of the project and its benefits, including how our developers can work best alongside a client’s existing team to ensure a smooth transition to the new system.

2.6 Experience of integrating CiviCRM with other applications

A[redacted]

t[redacted]

2.7 Our approach to testing and quality assurance

Our developers initially perform functional tests of their work against documentation on their dev environment. When developing CiviCRM extensions or Drupal modules we will use a combination of unit tests if applicable, functional tests as described in the documentation and will often produce Selenium tests to prevent regressions being introduced in future releases. We involve our support team in testing and documentation of functionality so that they are better able to support the software, but we rely on various members of the team to be involved in this crucial aspect of work, especially other developers and project managers.

3 Security

3.1 Protecting client data

Circle Interactive has ISO 27001 accreditation. As part of this accreditation process we have designed and implemented an Information Security Management System (ISMS) - a set of policies and procedures for systematically managing Circle's sensitive data. The goal of our ISMS is to minimise risk and ensure business continuity by pro-actively limiting the impact of a security breach. We can share the ISMS individual policies with HealthWatch England. Circle deal with sites that handle a wide range of sensitive and confidential data. Security, confidentiality and data-protection are at the heart of our thinking and we maintain strong security procedures around access to all our servers and data. We ensure amongst other things that systems are secure by design, strong passwords are in use by all our users, and all network traffic takes place over SSL. We only use UK hosting with extremely high physical data-centre security and some of our servers are PCI scanned to ensure compliance with e-commerce standards. Secure password protocols are observed and server passwords will adhere to good practice, using industry -standard levels of security (>15 characters and must include all of: upper and lower case a-z, numbers and special characters). Only permanent staff with sysadmin level of trust have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. Additionally we run regular technical briefings in which we ensure that all members of the development team and project managers are kept up to date with OWASP principles and that our development work is undertaken with these principles at its core.

3.2 Security vetting of staff

We follow the Basic Personnel Security Standard. We confirm ID from a passport or driving license with photo id, obtain references, and keep copies of these on record. If employing anyone who is not British we confirm their right to work through either EU citizenship, or work visa. We have recently brought in basic disclosure checks and are aware of the procedures for checking and recording date/relevant documentation when employing anyone from outside the EU.

3.3 Confidentiality procedures

We regard all data handled by us as confidential and will only use any client's data as part of troubleshooting or development. We will only keep versions of the database that we need for development and backup purposes and will delete all data not needed. All databases are held on

highly secure servers which require at least two levels of authentication to access and only allow access over secure (encrypted) connections. We will never store client data on laptops, USB sticks or other portable devices that could be removed from our office. All our staff are subject to non-disclosure and confidentiality agreements which covers all details of their work but especially data. Circle Interactive provide training to all employees to help them understand their responsibilities when handling data.Employees are required to request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection. Circle employees are required to keep all data secure, by taking sensible precautions and we issue the following guidelines:

• Strong passwords must be used and they should never be shared. (>15 characters and must include all of: upper and lower case a-z, numbers and special characters).
• Password managers should be used to enable the use of strong passwords.
• Personal data should never be disclosed to unauthorised people, either within the company or externally.
• The only people able to access data are those who need it for their work.
• Data should not be shared informally.
• When access to confidential information is required, employees are required to request it from their line managers.

Only permanent staff with sysadmin level of trust will have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. These policies apply to all Circle staff including temporary staff, hosted staff, contractor and secondees.

3.4 Access to data controls and potential breaches

Formal procedures are in place to control the allocation of access rights to information systems and services. These procedures cover all stages in the lifecycle of user access (from initial registration of new user accounts to deletion of access rights when user accounts are no longer required). Special attention is given to the allocation and management of privileged user rights but our basic principle is that the only people able to access data are those who need to for their work. We manage access to systems through a periodic review of the Information Security Management Team and this is implemented by the Sysadmin Team. Circle Interactive has in place an incident reporting mechanism that details the procedures for the identifying, reporting and recording of security incidents. Circle continually update and inform Circle staff of the importance of the identification, reporting and action required to address incidents, to ensure they are proactive in addressing these incidents as and when they occur. We foster a culture of proactive incident reporting and logging which we believe will help reduce the number of security incidents that could otherwise go unreported and unnoticed.

4 Service Management

4.1 Roles & responsibilities

The dedicated Service Management Team at Circle would typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Sysadmin – server infrastructure
Senior Developer – technical input as required
Support – escalated assistance via ticket/call
Others as necessary

We'd expect the HealthWatch England (HWE) Service Management Team to typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Support – 1st line HWE England support, escalating to Circle
Others as necessary

4.2 Standard service & performance reporting methods/frequencies

We always aim to offer our clients the level of support they need at regular preagreed intervals. The provision of these services will be pre-aligned to HealthWatch England's and their users needs. Services will be delivered to a defined quality, sufficient to satisfy requirements identified from business processes. A clear service portfolio will be developed and maintained as the basis for all service delivery and service management activities. For all services, a corporate level SLA and/or specific SLAs, which have been agreed with relevant stakeholders, will be in place. We will normally provide weekly phone updates on the progress of all development work, tickets and incidents. Resolved/completed issues will be further listed in billing and we maintain an ongoing spreadsheet of all support tickets resolved. This currently lists which tickets were closed during which month. Our internal monitoring also measures time to first response on tickets and numbers of tickets in certain statuses for more than a given time. We'd be happy to explore additional reporting that we can supply to HWE on your tickets.

4.3 Circle Service desk interface with HealthWatch England

1st line: HWE dedicated support, triage and deal with or escalate to Circle
2nd line: HWE support submit ticket to Circle support desk where it is dealt with by either Project Manager or Support team or escalated within Circle 3rd line: Escalate to developer/sysadmin

Performed during normal working hours 9am – 5pm UK time. Out-of-hours support services may be provided by prior arrangement. We will provide HWE with user accounts for our support site to enable the creation and tracking of support tickets through this interface and so you can upload images (such as screen shots) and other files relevant to the issue. We will monitor all tickets created through this system regularly throughout the working day. In the case of some issues where there is an element of particular urgency or a complication that is difficult to describe through a written report, we are available to discuss issues on the phone as well. We would expect this to normally be restricted to HWE staff but acknowledge that in some cases it may be sensible to include Local HW staff at HWE's discretion. For more urgent issues, or when a call may be more efficient to resolve an issue than an exchange on the ticket system, we will sometimes call your staff or take take their calls. We'd expect this to be an adjunct to the ticketing system so that information is still recorded there for reference.

4.4 Incident categorisation and management

As part of the ISO 27001 accreditation process, we have an Incident Management Policy giving clear guidance, policies and procedures and can share this policy with HealthWatch England. Along with this policy, Circle are fostering a culture of proactive incident reporting and logging to help reduce the number of security incidents that could otherwise go unreported and unnoticed. We have

monitoring in place that can trigger incident reporting and in cases of this, as well reporting the incident for our internal processes, we'll also notify your team. Circle's responsibilities and response to incidents:
• incidents are reported in a timely manner and are properly investigated
• incidents are handled by appropriately authorised and skilled personnel
• appropriate levels of management are involved in the determination of response actions
• incidents are recorded and documented
• the impact of the incidents are understood and action is taken to prevent further damage
• external bodies or data subjects are informed as required
• the incidents are dealt with in a timely manner and normal operations restored
• the incidents are reviewed to identify improvements in policies and procedures

5 Exit

During the course of the contract, we would maintain documents that will detail the technical infrastructure, support processes and development work undertaken. Transition may require the production of additional documentation and/or training for the in-coming provider and we'd provide this to whatever extent you determine is necessary as part of the contract. At the point where this contract would be terminated and taken over by another party or taken in-house, following written confirmation of the above, we would appoint a single person to act as the Exit Manager and this would likely be one of the main points of contact during the operation of the contract. The Circle exit manager and the HWE exit manager would between them draw up a plan and timetable for the transfer of documentation, winding down of any services and any interim management structure that may be needed to ensure a smooth transition with minimal disruption. If interim assistance is required during or after the termination of our main services, these would be agreed as part of the plan and timing and cost of these services would form part of the overall exit plan. Our exit manager would ensure that we would provide full cooperation and effect the transition with minimal disruption. In particular they would liaise with the exit manager from HWE and ensure that all documentation is properly listed and that the transfer of all assets takes place including but not limited to:
• any custom code base
• access to all code repositories
• access to all production servers and test environments
• notes and documentation relating to development
• support tickets
• backups
• any encryption keys and other cryptographic controls
• domains

During the course of our involvement with this project we have also set up contracts on behalf of HealthWatch England such as the contract for several dedicated and virtual servers and we would need to transfer those contracts to HealthWatch England or another party on exit or before this. Following transfer of all assets to their new controller and acceptance of that process, and following final cessation of the services we would then destroy all unnecessary records and data relating to this project, by shredding paper and securely wiping all digital copies ensuring in particular that no personal data remains on our systems. We would of course need to retain some records of work done and financial transactions for our internal reference and these would be kept in accordance with our record retention policy.

6 Discovery and research

This Lot requires a range of user research activities to compile a comprehensive understanding of the digital needs of the Healthwatch network including Healthwatch England. It will involve identification of the best digital products and solutions to transform the HW digital estate creating a sustainable digital support offer in line with the Healthwatch 5-year strategy. The type of work requires experience and understanding of a range of research techniques for gathering and analysis of research data, synthesis of findings, and presentation of clear findings that colleagues can understand and use. Circle do not have this type of expertise in house and would work with and support a third party specialist research organisation to undertake this piece of research. We would manage the work of the third party and coordinate their work with HWE.

7 Cost

The cost of of any development work undertaken as part of this lot will be charged at our standard day rate of £[redacted] and will be worked out on a project by project basis once details have been decided on and we're able to provide a clear estimate for the piece of work in question. Our estimate of the work required of a third party researcher to engage with the Healthwatch network and undertake the work needed is in the region of £[redacted] including the costs of Circle managing aspects of the work and supporting them in their work.

LOT 5 Development (Web) Response:

We are one of the UK's leading open source specialist agencies with strong technical and design skills and wide experience of consulting on, implementing, hosting and supporting a range of complex community websites. We have been working with Drupal and CiviCRM since 2006 and currently support well over a hundred clients on this platform, including NGOs and charities, international corporations, Local Infrastructure Organisations, educational institutions, a political party and a UN agency. We believe that the breadth of our experience and depth of our knowledge makes us ideally placed to undertake this project. We are very excited about the possibility of working with HealthWatch and believe we could continue to provide you with an effective, scalable and future-proof CRM that will be easy to maintain.

[redacted]

1 Overview

The key partners in the business, [redacted]ave been working together for more than fifteen years now and most of the other members of the team are experienced professionals who have been in the industry for a similar length of time. We are based in Bristol but have clients all over the UK, Europe and beyond. We aim to develop long term working relationships with our clients, supporting their development and adding new features to their websites and contact databases as they become more sophisticated users of those systems. Our preference is to work with open source software, as this provides cost benefits, better security and faster development times. We feel this is particularly relevant when working with publicly funded organisations where not just value for money is paramount but where the ethos of sharing knowledge is part of the value system.

We specialise in building and consulting on complex Drupal and CiviCRM systems and have been regular contributors to both projects but especially CiviCRM with performance optimisations, bug-fixes, core code updates and sponsored features. We have completed over two hundred projects based on this platform to create systems to manage publishing, membership organisations and communities, e-commerce platforms, service delivery monitoring and more: for commercial clients the public and third sectors. We currently provide hosting, support and elements of the development plan for HealthWatch and have been involved in this project since 2013. We think our proven ability to bring to the table our extensive knowledge of these excellent open source products and experience of working with HealthWatch England makes us ideally placed to collaborate on this project. Our knowledge of the Local HealthWatch network gained from early stage interviews and on-site visits gives us insights in their needs and issues that can be extremely valuable when planning and implementing future development. We build websites, intranets, back office systems and complex community portals. [redacted]

CiviCRM database allowing various levels of access, moderation and control to a highly complex system with tens of millions of records and hugely varied reporting requirements. [redacted] o[redacted] on leaving his post: It's been an immense pleasure to work with you over the past few years and frankly I believe you have been instrumental in the amazing success that we've achieved over that time. Your patience, counsel, advice and support has always been of tremendous value and I don't think we would have made anywhere near the progress we have done without your help.

Projections for company growth

Circle is a stable company established in 2005 that has grown steadily in that time mainly through our reputation as leaders in expertise with CiviCRM. Last year we turned over about [redacted]with a profit of [redacted] This year we expect that to increase to around [redacted]with a slightly increased margin. We've built up a client base of over 150 organisations including a political party, several well know large charities, many smaller ones plus a range of private businesses and public sector organisations. We have the largest team of experienced CiviCRM developers based in the UK and are looking to continue our recent growth of between [redacted] Core to this growth are three strands of our business:

- development of new functionality that we share between groups of sites,
- a stable and highly secure hosting environment based in the UK,
- a responsive technical support desk.

As well as providing these services to our clients directly, we also support several independent Drupal / CiviCRM consultants with our hosting and support and sometimes technical elements of development work that they feel we can undertake more effectively than they can. Part of our strategy is to continue to expand these relationships, working collaboratively with others in both Drupal and CiviCRM communities. Our growth plans also include the provision and maintenance of product-like software distributions for certain vertical markets allowing us to build on expertise with e.g. medical associations to provide a platform that several organisations can use and develop with benefits going to all. This is something we've been building gradually over the last few years and which is expanding as a percentage of our turnover.

Key to our ability to scale up from this position is reviewing our processes and for several months now we've been undergoing a major initiative to document and review all processes, improving those where there is scope to increase efficiency by having further cross-team involvement.

2 Development

2.1 Experience of providing Drupal development capability

We've been working with Drupal for over 10 years building complex e-commerce systems dedicated publishing and discussion forums for members and providing front-end and back -end customisations. We've worked on Drupal since version 4 and while most of work is still focussed on Drupal 7, we are currently working on Drupal 8 systems that allow a single editing tool to be used for pushing content to a series of highly secure front end web-sites. We've built over about 250 Drupal based websites, some for temporary projects, some that have evolved over time and gone through several transformations as the operating organisations have grown in complexity and size or changed their focus. Many are linked with news feeds populating multiple sites from a single source and the majority give users of varying roles the ability to interact with the site in some way: posting comments or submitting news and events for approval and so on. We have worked with

organisations such as AbilityNet, RNIB and Dyslexia Action to produce highly accessible sites that conform to the highest standards.

2.2 Delivery of new functionality in Drupal

Some examples of our experience of developing features using Drupal:

Organisation manager – allows an organisation's designated manager to update new staff, remove ex-staff and allocated permissions to the existing staff list. This uses Organic Groups and CiviCRM and is designed for organisations whose members or partner organisations will have multiple users logging in to and interacting with the site at different permission levels.

Support – this has extended the support module to allow for multiple members of a client team to interact on support tickets while allowing support team members to exchange private notes and change the status of the ticket from the comment form.

Quote manager – allows users to submit their details to an insurer who can then issue quotes that the users have to sign accept before going through to pay. The insurer then issues a certificate with the details through the system.

Grant application manager – allows users to save drafts of their application form while building up all the evidence needed to submit. Then puts the application into a holding state while it is assigned to several assessors who score it. Applications with sufficient scores are then moved on to the next round and the original applicant is asked for further details before a more in-depth assessment is made.

3. Experience of developing Drupal sites for complex organisations Making Music

Content editors add site content and moderate posts, while end users can update their profiles and add events. Amateur groups also purchase insurance through the site and the insurers issue insurance quotes which the Groups accept before the insurers take payment and issue certificates through the site. Editors and groups also update the Music Bank database of sheet music and offer copies for loan.
https://www.makingmusic.org.uk/
https://www.makingmusic.org.uk/resources/music-bank

Bristol Green Doors

Content editors, home owners and service providers all log into the site with different views of the system and the ability to update their own published information. In the case of home owners this is added to the searchable database.
http://www.bristolgreendoors.org/

Green Party

Content writers, moderators, national party officers, policy team, local party secretaries, members, and more all contribute to the various content at national, regional and local levels on this site, where members not only manage their memberships but join in the conversation at different levels. https://my.greenparty.org.uk/

Arts Professional

Arts Professional have site editors, freelance writers and commissioning editors. Site editors add stories to the site under the direction of the commissioning editors and this is published immediately. Freelance writers and requested to write a piece by the commissioning editors, submit drafts for feedback and eventual approval before the editor publishes it to the site. All workflows are managed in Drupal. Users can also login to post on the site and related tweets are added to content.
http://www.artsprofessional.co.uk/

2.4. Approach to development & engagement in the wider community

We are active members of the community, providing financial and time inputs, sponsoring events and sending people to sprints to contribute code revisions. We contribute code and testing time, collaborate on the development of extensions, writing some ourselves, adding to and improving on others. We also contribute code and testing time to most releases of the product and are actively involved as part of the security team.

2.5 Development of applications using Agile methodologies

Our preferred methodology for application development is to always take an Agile approach and we hold periodic workshops for the whole development team to ensure our approach constantly improves. Our framework allows for flexibility and focusses on the practical consequences of any work as it will affect the delivery of the finished product. Working in an agile way does sometimes require a cultural shift in some client organisations because it focuses on the clean delivery of individual pieces or parts of the software and not on the entire application. It also guarantees cost, delivery time, and quality but not outcomes. Our methodology involves aspects of Scrum and XP but adapted to suit the nature of the type of projects we typically work on. We plan sprints of a suitable time for the chunk of work being undertaken – typically 2 to 3 weeks. We will always have a working piece of software at the end of that sprint for review though not all elements may be complete. We often work in XP style pairs with two pairs of eyes on the code to ensure quality and aid us in security planning. We do daily stand-ups though we don't religiously document the backlog on smaller projects where this would add unduly to the admin overhead. We use MoSCoW prioritisation and time boxing to ensure the key features are delivered according to the plan.

Planning Phase (Facilitated Workshops)

We think the most important step in any major database change is the planning phase. Without effective, strategic planning aligned to organisational goals, a project will often go ‘off the rails’ and end up exceeding both the expected time limit and budget. At Circle, we like to take our clients through an extensive ‘discovery’ process, where we gather as much relevant information about the proposed workflows and anticipated benefits as we can. We then have a clear sense of the project and its benefits, including how our developers can work best alongside a client’s existing team to ensure a smooth transition to the new system.

2.6 Experience of integrating Drupal with other applications

This is one of our areas of particular expertise and over the years we have built dozens of integrated systems apart from the >100 CiviCRM integrations which range in complexity from simple to extremely complex. In particular we've integrated data and access levels with:

Moodle: We've undertaken several integrations with this online virtual learning environment. These have been mostly single sign ons allowing users to access the Moodle once logged on to the Drupal site where their profile would be stored along with any blogs and forum posts.

SCRAN: www.scran.ac.uk We integrated a community site with this existing platform for a project by Dyslexia Action in conjunction with RNIB. Users logged into the SCRAN system and were able to see some details from their Drupal presence while clicking through in a SSO environment to update those details and take part in discussions on the Drupal.

TT Exchange: We've integrated the https://www.tt-exchange.org/ Drupal with a custom application built around CiviCRM by TechSoup which monitors various licencing agreements they have with large vendors such as Microsoft. SCIE: We built a system that integrated with SCIE's proprietary CMS to allow data syncing across various fields as users applied for grants through a series of Drupal forms, had their profiles listed from SCIE and updated while their application took place through a mix of CiviCRM's Case management and customised Drupal webforms.

2.7 Experience of migrating content from other CMS solutions into Drupal

Many of our projects involve this type of work and we've undertaken scores of content migrations including
WP → Drupal 7 using feeds
WP → Drupal 7 using Drupal modules
Joomla! → Drupal using custom code and SQL queries
Earlier Drupal versions to later Drupal versions using SQL queries (D6→ D7, D7 → D8)
Other database driven CMS via db queries
Other database driven CMS and static sites via scraping tools that dump page content into the database via a parsing tool that finds markers in the content and puts content into the relevant fields from this.

2.8 HealthWatch Drupal template rollout

If these were to be hosted centrally like the CRM, then consistency can easily be guaranteed. We would recommend setting up the whole site as an install package maintained in version control including 'features', sets of contributed modules and a theme with accompanying templates which can then be very simply updated and tested through a normal git workflow and deployed to the various sites using a series of ansible scripts from the master branch of the git repository.
This is how we are currently operating and any further developments whether small design changes or significant additions of functionality can be committed to the code base, deployed to a staging instance for testing, and subsequently deployed to the entire network of production instances.
The install package also means it's easy to deploy a new instance using the latest version of the site, containing all templates, content and features when each new LHW requests to be included.

2.9 Our approach to testing and quality assurance

Our developers initially perform functional tests of their work against documentation on their dev environment. When developing CiviCRM extensions or Drupal modules we will use a combination of unit tests if applicable, functional tests as described in the documentation and will often produce Selenium tests to prevent regressions being introduced in future releases. We involve our support

team in testing and documentation of functionality so that they are better able to support the software, but we rely on various members of the team to be involved in this crucial aspect of work, especially other developers and project managers.

2.10 Approach to sharing industry knowledge

We would recommend a regular (perhaps quarterly or half yearly review of plans and feedback in order to discuss ideas coming from the network and look at how some of these might be incorporated into the offering: which would be easy to implement and which more challenging so that prioritisation can be done by HWE. We'd recommend that in these sessions, time is also allocated for us to provide thoughts on next steps and interesting developments. There are a couple of decisions which we think will be needed over the coming year or so. One will be to review the potential integration between the CiviCRM instances and the public facing websites. Another will be the approach to upgrading Drupal 7 to Drupal 8 or possibly skipping this and moving to Drupal 9. This kind of strategic decision requires the kind of time and space not currently allocated in the ongoing development and maintenance programme but which will need to be dealt with before too long.

3 Security

3.1 Protecting client data

Circle Interactive has ISO 27001 accreditation. As part of this accreditation process we have designed and implemented an Information Security Management System (ISMS) - a set of policies and procedures for systematically managing Circle's sensitive data. The goal of our ISMS is to minimise risk and ensure business continuity by pro-actively limiting the impact of a security breach. We can share the ISMS individual policies with HealthWatch England. Circle deal with sites that handle a wide range of sensitive and confidential data. Security, confidentiality and data-protection are at the heart of our thinking and we maintain strong security procedures around access to all our servers and data. We ensure amongst other things that systems are secure by design, strong passwords are in use by all our users, and all network traffic takes place over SSL. We only use UK hosting with extremely high physical data-centre security and some of our servers are PCI scanned to ensure compliance with e-commerce standards. Secure password protocols are observed and server passwords will adhere to good practice, using industry-standard levels of security (>15 characters and must include all of: upper and lower case a-z, numbers and special characters). Only permanent staff with sysadmin level of trust have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. Additionally we run regular technical briefings in which we ensure that all members of the development team and project managers are kept up to date with OWASP principles and that our development work is undertaken with these principles at its core.

3.2 Security vetting of staff

We follow the Basic Personnel Security Standard. We confirm ID from a passport or driving license with photo id, obtain references, and keep copies of these on record. If employing anyone who is not British we confirm their right to work through either EU citizenship, or work visa. We have recently brought in basic disclosure checks and are aware of the procedures for checking and recording date/relevant documentation when employing anyone from outside the EU.

3.3 Confidentiality procedures

We regard all data handled by us as confidential and will only use any client's data as part of troubleshooting or development. We will only keep versions of the database that we need for development and backup purposes and will delete all data not needed. All databases are held on highly secure servers which require at least two levels of authentication to access and only allow access over secure (encrypted) connections. We will never store client data on laptops, USB sticks or other portable devices that could be removed from our office. All our staff are subject to non-disclosure and confidentiality agreements which covers all details of their work but especially data. Circle Interactive provide training to all employees to help them understand their responsibilities when handling data. Employees are required to request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection. Circle employees are required to keep all data secure, by taking sensible precautions and we issue the following guidelines:

• Strong passwords must be used and they should never be shared. (>15 characters and must include all of: upper and lower case a-z, numbers and special characters).
• Password managers should be used to enable the use of strong passwords.
• Personal data should never be disclosed to unauthorised people, either within the company or externally.
• The only people able to access data are those who need it for their work.
• Data should not be shared informally.
• When access to confidential information is required, employees are required to request it from their line managers.

Only permanent staff with sysadmin level of trust will have access to the servers. All Circle staff are subject to Confidentiality Agreements at least as stringent as we have with our clients. These policies apply to all Circle staff including temporary staff, hosted staff, contractor and secondees.

3.4 Access to data controls and potential breaches

Formal procedures are in place to control the allocation of access rights to information systems and services. These procedures cover all stages in the lifecycle of user access (from initial registration of new user accounts to deletion of access rights when user accounts are no longer required). Special attention is given to the allocation and management of privileged user rights but our basic principle is that the only people able to access data are those who need to for their work. We manage access to systems through a periodic review of the Information Security Management Team and this is implemented by the Sysadmin Team. Circle Interactive has in place an incident reporting mechanism that details the procedures for the identifying, reporting and recording of security incidents. Circle continually update and inform Circle staff of the importance of the identification, reporting and action required to address incidents, to ensure they are proactive in addressing these incidents as and when they occur. We foster a culture of proactive incident reporting and logging which we believe will help reduce the number of security incidents that could otherwise go unreported and unnoticed.

4 Service Management

4.1 Roles & responsibilities

The dedicated Service Management Team at Circle would typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Sysadmin – server infrastructure

Senior Developer – technical input as required
Support – escalated assistance via ticket/call
Others as necessary

We'd expect the HealthWatch England (HWE) Service Management Team to typically consist of:
Project Director – strategic
Project Manager – day to day management & communications
Support – 1st line HWE England support, escalating to Circle
Others as necessary

4.2 Standard service & performance reporting methods/frequencies

We always aim to offer our clients the level of support they need at regular preagreed intervals. The provision of these services will be pre-aligned to HealthWatch England's and their users needs. Services will be delivered to a defined quality, sufficient to satisfy requirements identified from business processes. A clear service portfolio will be developed and maintained as the basis for all service delivery and service management activities. For all services, a corporate level SLA and/or specific SLAs, which have been agreed with relevant stakeholders, will be in place. We will normally provide weekly phone updates on the progress of all development work, tickets and incidents. Resolved/completed issues will be further listed in billing and we maintain an ongoing spreadsheet of all support tickets resolved. This currently lists which tickets were closed during which month. Our internal monitoring also measures time to first response on tickets and numbers of tickets in certain statuses for more than a given time. We'd be happy to explore additional reporting that we can supply to HWE on your tickets.

4.3 Circle Service desk interface with HealthWatch England

1st line: HWE dedicated support, triage and deal with or escalate to Circle
2nd line: HWE support submit ticket to Circle support desk where it is dealt with by either Project Manager or Support team or escalated within Circle 3rd line: Escalate to developer/sysadmin

Performed during normal working hours 9am – 5pm UK time. Out-of-hours support services may be provided by prior arrangement. We will provide HWE with user accounts for our support site to enable the creation and tracking of support tickets through this interface and so you can upload images (such as screen shots) and other files relevant to the issue. We will monitor all tickets created through this system regularly throughout the working day. In the case of some issues where there is an element of particular urgency or a complication that is difficult to describe through a written report, we are available to discuss issues on the phone as well. We would expect this to normally be restricted to HWE staff but acknowledge that in some cases it may be sensible to include Local HW staff at HWE's discretion. For more urgent issues, or when a call may be more efficient to resolve an issue than an exchange on the ticket system, we will sometimes call your staff or take take their calls. We'd expect this to be an adjunct to the ticketing system so that information is still recorded there for reference.

4.4 Incident categorisation and management

As part of the ISO 27001 accreditation process, we have an Incident Management Policy giving clear guidance, policies and procedures and can share this policy with HealthWatch England. Along

with this policy, Circle are fostering a culture of proactive incident reporting and logging to help reduce the number of security incidents that could otherwise go unreported and unnoticed. We have monitoring in place that can trigger incident reporting and in cases of this, as well reporting the incident for our internal processes, we'll also notify your team. Circle's responsibilities and response to incidents:

• incidents are reported in a timely manner and are properly investigated
• incidents are handled by appropriately authorised and skilled personnel
• appropriate levels of management are involved in the determination of response actions
• incidents are recorded and documented
• the impact of the incidents are understood and action is taken to prevent further damage
• external bodies or data subjects are informed as required
• the incidents are dealt with in a timely manner and normal operations restored
• the incidents are reviewed to identify improvements in policies and procedures

5 Exit

During the course of the contract, we would maintain documents that will detail the technical infrastructure, support processes and development work undertaken. Transition may require the production of additional documentation and/or training for the in-coming provider and we'd provide this to whatever extent you determine is necessary as part of the contract. At the point where this contract would be terminated and taken over by another party or taken in-house, following written confirmation of the above, we would appoint a single person to act as the Exit Manager and this would likely be one of the main points of contact during the operation of the contract. The Circle exit manager and the HWE exit manager would between them draw up a plan and timetable for the transfer of documentation, winding down of any services and any interim management structure that may be needed to ensure a smooth transition with minimal disruption. If interim assistance is required during or after the termination of our main services, these would be agreed as part of the plan and timing and cost of these services would form part of the overall exit plan. Our exit manager would ensure that we would provide full cooperation and effect the transition with minimal disruption. In particular they would liaise with the exit manager from HWE and ensure that all documentation is properly listed and that the transfer of all assets takes place including but not limited to:

• any custom code base
• access to all code repositories
• access to all production servers and test environments
• notes and documentation relating to development
• support tickets
• backups
• any encryption keys and other cryptographic controls
• domains

During the course of our involvement with this project we have also set up contracts on behalf of HealthWatch England such as the contract for several dedicated and virtual servers and we would need to transfer those contracts to HealthWatch England or another party on exit or before this. Following transfer of all assets to their new controller and acceptance of that process, and following final cessation of the services we would then destroy all unnecessary records and data relating to this project, by shredding paper and securely wiping all digital copies ensuring in particular that no personal data remains on our systems. We would of course need to retain some records of work

done and financial transactions for our internal reference and these would be kept in accordance with our record retention policy.

7 Cost

The cost of of any development work undertaken as part of this lot will be charged at our standard day rates of [redacted] and will be worked out on a project by project basis once details have been decided on and we're able to provide a clear estimate for the piece of work in question.

Scenario Lot 3 and 5

This scenario covers aspects of Lot 3 (CiviCRM) and Lot 5 (Drupal website). Currently we run separate platforms for our websites and CiviCRM instances although this may change so the resulting module must provide flexibility to accommodate several scenarios.

Drupal module

The module must be capable of acting as a standalone system should the user not have a CiviCRM installation. The module should also allow for integration with a CiviCRM installation should it be available on the website installation. The module can:

- operate as a standalone module
- be integrated into a CiviCRM should one exist
- be rewrapped for use on other platforms (i.e. WordPress…)

Styling

The module must sit on the existing website template and theme system. The result will be that any changes to the theme (visual element) of the website should simply be adopted by the system provided.

Survey tool

Enhancements to the current CiviCRM system to enable it to collect information on a survey basis through code enhancement or a Drupal module. SurveyMonkey is the bar set for flexibility and features.

- Locked fields (currently 11): The 11 fields would need to be locked from users of the system being able to alter them. Whilst this is a locked set of fields it must be possible to add or remove from this list provided the user account has high enough permissions to do so.
- Free fields: the users of the system would need to be able to add their own fields on top of the existing fixed fields mentioned above. The number of fields should be flexible without additional developer interference.
- Some fields may be created based on other fields values (for data connectivity and export).

Data connectivity

The module should have the facilities to allow the user to collect data in a number of ways. The standalone system should allow for data to be exported in a CSV/Excel format for later processing by the owning organisation.

Where a CiviCRM installation exists, the data would be sent through to the system.

The ability to allow for “Locked fields” data to be sent to HWE CiviCRM via the API or other central database system.

- CSV/Excel export
- Straight to CiviCRM
- API connectivity to HWE CiviCRM or other database system

Accessibility
The system must comply to accessibility standard W3C and be compatible across devices (Desktop, tablet, phone)

Response

Whether the site has a CiviCRM installation or not, there will need to be a survey tool and the Drupal Webform module is the most sensible starting point for this. It's a highly flexible tool that is maintained as part of Drupal's security policy and has a similar level of functionality to Survey Monkey although with the advantage that his can be extended either with Drupal's Rules (another Drupal contrib module) or with further custom code in “helper” modules. Additionally, Webform integrates directly with CiviCRM and has the option of pushing data directly into a CiviCRM db connected to the Drupal. Webform is in fact the basis of the “Wizard” used for collecting activity data by HW currently and in this case there is some customisation in place to allow for some elements of the workflow that could not be accommodated “out of the box”.

One significant advantage of the Webform module is that it will pick up the default site styling although it is not uncommon for some minor tweaks to be needed to fine tune the layout of the form. This would normally not amount to more than half a day or so of work, testing and deployment. However, it would be prudent to allow for some additional time to focus on the permissions allocated to the various roles that might interact with this form, both creating it and submitting from the ned user perspective.

Accessing fields
For the form to access fields that are currently represented in CiviCRM, the Drupal instance would need to be connected to a CiviCRM instance so this would be able to pick up the field IDs and options. If some sites would not have a CiviCRM install at all and given the current separation of Web and CRM instances, this should probably be a dummy install which doesn't contain real data but has the field sets available for the form to refer to. In this way, users with the correct permissions would be able to select from the fields in use in the actual CiviCRM instances as outlined.

It may be that as part of this exercise, a review of the separation between Drupal and CiviCRM should be undertaken for the hosted LHW sites.

Locked fields
There is in existence on the HW CiviCRM sites an extension developed by Circle which allows certain fields in the database to be locked in CRM. That is to say, no user except with the highest permissions can edit the names of these fields, disable them or change the options, format etc.

These fields are used not just in the LHW CiviCRM instances but are part of the data set pushed to HWE CiviCRM on submission of the Wizard.

These fields are currently determined in code in the extension and there is no admin interface. In order to allow some users with the correct roles and permissions to add to or amend this list, would require exposing the list to the User Interface and this would require about 40-50 hours of work, testing and deployment to the network.

In order to simply lock some of the fields in the Webform would be simpler. This would require a “helper module” for the webform which would define a basic set of fields as uneditable. Such a module exists in the form of Webform Default Fields https://www.drupal.org/project/webform_default_fields but we think this will not have all the functionality required to lock the fields in conjunction with CiviCRM as outlined here so some further development would be required and we estimate in the order of 60-80 hours work to integrate this and ensure that the fields locked through the CiviCRM extension become locked in the Webform. There would need to be locking on a level that the administrator could not override for those fields.

Additional Fields

For administrators to add fields to their own Survey through the Webform module would be unproblematic for those sites with no CiviCRM instance. Those fields could simply be added to the webform through the normal interface. This is part of the functionality of Webform.

However, for sites that have a CiviCRM, they would need to add their additional fields to their CiviCRM instance for those fields to be useful to them. In this case, we'd need a mechanism to get the additional fields showing up in the local Webform so they could choose them to appear in the survey tool. A simple way of doing this would be to write something that would lookup the corresponding CiviCRM (if it exists) take a dump of certain CiviCRM tables (those that contain the custom fields and ensuring that it ignores any actual contact data) and update the dummy CiviCRM instance from that. In this way, fields added to the CiviCRM through that UI would become available in the webform. This would require about 24 hours work to develop, test and deploy.

Data output to CSV

This is a standard option with both Webform and Caldera Forms so only local configuration would be required.

Data push to LHW CiviCRM

Where there is a CiviCRM instance, we'd need a mechanism to identify this (already proposed in the migration of fields) and a connector to push the data into this instance. A few hours of work would see the connect working both ways to identify whether a CiviCRM instance exists or not. Pushing the data to this would require something similar to the existing Data Push Module which currently pushes data submitted directly into CiviCRM across to the HWE CiviCRM instance.

Data output to HWE via API

The current data push module which pushes form submissions from LHW CiviCRM instances into the HWE CiviCRM would be a good starting point for this functionality. It already deals with authentication and deals with failures through notifications so members of the team can investigate and amend entries to enable the push to happen correctly. The API endpoint for this would thus

work in principle. Some adjustment may be needed to get what is essentially a less controlled data set to flow through. However, the data -push extension already only picks out certain fields for push to HWE so it should only need to take into account the fact that this list should come from the newly proposed UI interface rather than the current hard coded list. That is likely to be a couple of days work.

There will also need to be some adjustment to the trigger mechanism. Currently this happens on submission of a particular webform, but that would simply need to be extended to take account of the new webforms which could be multiple and changing.

If the end point of the data push were to be no longer the HWE CiviCRM, some additional work would be needed to make the data flow into the replacement database. It's impossible to estimate with any degree of accuracy something with so little certainty, but it's reasonable to assume that a couple of weeks work would be needed for an exercise of this kind and it would need include mapping the current data fields to their new locations and changing the queries needed to push the data into its newly mapped fields in that replacement database.

Accessibility

The current website accessibility standards would apply to the new form as this would be delivered through a Drupal template using the same styling and templates. The only cost for this would be some additional testing.

Wordpress

Wordpress has a similar webform type Plugin that integrates with CiviCRM called Caldera Forms. The code to replicate the CiviCRM instances would remain unchanged as this would be implemented as a server level script. The data-push changes would need to be amended to take the submission of the Wordpress Caldera form as a trigger, but otherwise nothing much would need to change on that front. However, the whole structure of Drupal Modules and Wordpress Plugins is somewhat different and there would need to be an exercise in porting this from one platform to the other. Since most of the code operates behind the scenes of actually talking to Drupal (or Wordpress) but is involved in the extraction of CiviCRM data and pushing that htrough an API call into another database, the porting should not be too bad and we'd maybe allow for a couple of weeks of additional work to undertake this, including some extensive testing.

Schedule 2 – Call-Off Contract charges

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

- Lot One Hosting and Maintenance - [redacted]
- Lot Two Support - [redacted]
- Lot Three CRM Development – to be split out as
  a) User Research - u[redacted]
  b) CRM Development - [redacted]
- Lot Five Web Development - £[redacted]

Current day rate [redacted]

Costs include VAT and the total contract amount is £312,407

Schedule 3 – NOT USED

Schedule 4 - NOT USED

Schedule 5 – NOT USED

Schedule 6- Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.

Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; iii) (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.

Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans

Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.11 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security Management Plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.

Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1 - Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are: **Nimali De Silva, 3rd Floor 151 Buckingham Palace Road, London SW1W 9SZ.**

1.2 The contact details of the Supplier's Data Protection Officer are: **Dave Morton, 1 Osbourne Road, Southville, Bristol, BS3 1PR**

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: ● Personal data held on the system that has been created or obtained by the Buyer for the exercise of the functions of the Buyer. The system will process personal data including name, address, date of birth, addresses, email telephone numbers, images, personal medical information and IP addresses. The parties acknowledge that for the purposes of the Data Protection Legislation, the Buyer is the Processor and the Supplier is the Sub-Processor of the following Personal Data: ● Personal data held on the system that has been created or obtained by a Local Healthwatch Organisation ("LHW") for the exercise of their own functions and which is processed on the system under contractual agreement with the Buyer. The system will process personal data including name, address,

	date of birth, addresses, email telephone numbers, images, personal medical information and IP addresses. The Supplier will process all of these data under, and in strict accordance with, instruction from the Buyer, so does not need to differentiate between the former and the latter for the practical purposes of fulfilling this contract. It is the Buyer's responsibility to ensure that instructions given to the Supplier in the role of Processor to Sub-Processor are lawful and in accordance with their own obligations to the relevant Local Healthwatch Organisation.
Duration of the Processing	01/10/2019 - 31/03/2021
Nature and purposes of the Processing	Healthwatch England ("HWE") has been established under the Health and Social Care Act 2012 ("the 2012 Act") to be the consumer champion for health and social care in England. Its purpose is to strengthen the collective voice of patients and users of health and social care services and of the general public. Under Section 45A of the Health and Social Care Act 2008 (as amended by the 2012 Act) has a function of providing general advice and assistance to LHW in relation to the carrying out of LHW's functions. To assist HWE and LHW in carrying out its functions, HWE has made an offer to provide, administer and support a website and CRM for the use of HWE and LHW. CQC on behalf of HWE has contracted Circle Interactive Limited to carry out the provision, administration, support and maintenance of this website and CRM. This document sets out the instructions of LHW to HWE, and via HWE to Circle Interactive Limited, regarding the processing of personal data by HWE to the extent required for the provision, administration, maintenance and support of this website and CRM.

Type of Personal Data	HWE and LHW will decide if and how the website and CRM are used to process personal data and special category personal data. Depending upon the decisions made by HWE and LHW, the following types of personal data may be processed under this agreement: • Identifying information (including names, initials, dates of birth, online identifiers, unique identifiers (such as NHS numbers). • Contact information (including addresses, postcodes, email addresses, telephone numbers). • IP addresses and tracking information (such as information collected via cookies). • Images, moving images, audio recordings. • Medical information, including information about people's experiences of the care and treatment provided by health and social care services. • Equalities monitoring information (including information about disabilities, physical and mental health, racial or ethnic origin, religious or philosophical belief, sexual orientation). • Other information that users of the website may choose to share with LHW via the website.
Categories of Data Subject	The website and CRM will process data related to LHW, HWE and CQC staff, volunteers, members of the public (including people who use health and social care services in England), providers of health and social care services and their staff, volunteers and other agents, commissioners and other stakeholders.
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	Upon the ending or termination of this agreement, or upon the request of LHW or HWE, or upon reaching a retention deadline for specific data set by LHW or HWE, Circle Interactive Limited will securely delete the data. Circle Interactive Limited and its sub-contractors/sub-processors will not retain, copy, use or otherwise process the personal data for any purpose other than as necessary to provide, support and administer the website and CRM on behalf of LHW and HWE.

Annex 2 - NOT USED

Part B - Terms and conditions

1. Call-Off Contract start date and length

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

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

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

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)

- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at schedule 7 of this Call-Off Contract.

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

5. Due diligence

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud

Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

- a broker's verification of insurance
- receipts for the insurance premium
- evidence of payment of the latest premiums due

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

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

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

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

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

- premiums, which it will pay promptly
- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.78 to 8.86. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

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

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

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

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

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

- rights granted to the Buyer under this Call-Off Contract
- Supplier’s performance of the Services
- use by the Buyer of the Services

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

- modify the relevant part of the Services without reducing its functionality or performance
- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

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

- the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract
- other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

- comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data
- only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
- take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

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

including by:

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- providing the Buyer with any information requested by the Data Subject

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

13. Buyer data

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

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

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

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

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

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

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets at https://www.cpni.gov.uk/protection-sensitive-information-and-assets

- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/collection/risk-management-collection
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

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

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

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

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

14. Standards and quality

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

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

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

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the

services have the relevant PSN compliance certification.

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

15. Open source

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

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

- an executed Guarantee in the form at Schedule 5
- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

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

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

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

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

- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- an Insolvency Event of the other Party happens
- the other Party ceases or threatens to cease to carry on the whole or any material part of its business

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

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

19. Consequences of suspension, ending and expiry

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

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

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date

(whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

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

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)
- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

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

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

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

otherwise.

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

20. Notices

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

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

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

21. Exit plan

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

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

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

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

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with

the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

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

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

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

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

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

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

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

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

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

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the

amount in the Order Form

25. Premises

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

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

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

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

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

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

26. Equipment

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

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

- the activities they perform
- age
- start date
- place of work
- notice period

- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

- work proactively and in good faith with each of the Buyer's contractors
- co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.57 and 8.58 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.57 and 8.58 are reproduced in this Call-Off Contract document at schedule 7