**Order Schedule 20 (Order Specification)**

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Order Contract

#

# Background to requirement/OVERVIEW of requirement

## GCSI has been building its Digital Learning capability over the last three years. To deliver digital learning effectively, GCSI must be able to offer courses online via a high quality digital platform Our current offering is built using an instance of edX, a massive open online course (MOOC) provider that supports open source development. To maintain the service to users we need support in hosting, maintaining and updating our edX instance and related open source components that make up our learning platform.

* 1. The service comprises an Open edX (currently Lilac version) application. Extensions have been developed for a custom theme, enhancements to the API and improvements to the Gradebook.
	2. An administration service for user and course booking management (GCAS\*) has also been built in Python Django, with a MySQL database for data storage.
	3. The services have been built using an infrastructure as code (IaC) approach with GitHub Actions, Terraform and Helm and deployed to a Kubernetes (EKS) based AWS platform with multiple environments such as Development, Test, Staging and Production.
	4. The service sees an average annual usage of 1 - 5000 users globally.

# definitions

|  |  |
| --- | --- |
| AAcronym | Definition |
| GCS | Government Communication Service |
| GCSI | Government Communication Service International |
| GCAS | Global Communications Academy System (the system commissioned by the Global Communications Academy) |
| EdX | Education X – learning platform |
| CO | Cabinet Office or the Contracting Authority |

#

# scope of requirement

## GCSI is looking for a Supplier to provide hosting and maintenance support for our digital learning platform.

## GCSI is looking for bidders to provide a summary of their proposed delivery approach, as well as details of their experience working with edX in other comparable learning contexts.

### Bidders should include a portfolio of credentials outlining their evidence of past project delivery in this field within their tender proposals.

# The requirement

* + 1. The initial contract term is 12 months, with an option to extend up to 6 months.

## **Hosting requirement**

## The Supplier must be able to provide us access to a dedicated server environment, hosted within the UK

## The Supplier must offer a service that minimises downtime, by committing to a service offering 99.8% or higher uptime. Any expected downtime must be communicated in advance in writing. Any unexpected downtime must be communicated in writing within 24 hours of the downtime occurring.

## **Maintenance and support requirement**

* + 1. The Supplier will also be responsible for providing technical support for the instance according to mutually agreed SLAs, e.g.

|  |  |  |
| --- | --- | --- |
| **Category** | **Description** | **Required Resolution Time** |
| Category 1: major time-sensitive issue | Code issue, service outage, performance issue, other major outage affecting multiple users | 4 business hours |
| Category 2: minor time-sensitive issue | Performance issue affecting one or small group of users | Within 1 business day |
| Category 3: non time-sensitive issue | User-identified platform issues (non-critical), user support queries, functionality or development requests | Within 3 business days |

## **Development requirement**

* + 1. The Supplier agrees to supply development resources to support a range of requests up to an agreed capped amount of work per year. The type of requests could include: edX version upgrades, additional functionality requests to gradebook or other bespoke aspects, configuration requests (e.g. integrating H5P), improvement of usability and UI of edX components, data aggregation and analysis. Discussion and costing of requirements to be negotiated at the point of need.

## **Technical capability requirement**

* + 1. The Supplier will demonstrate technical capability sufficient to maintain and improve on our current operational platform (including experience of AWS services, utilising a Kubernetes containerised environment, Open edX) A full list of core capabilities required can be provided upon request.
	1. **Platform requirements and User Interface**

## Technology and infrastructure capability vary within the geographical regions in which our users are based. The Authority therefore requires the platform to be cloud-based in order to provide the greatest flexibility for user access.

## The platform must support industry and [WCAG 2.1 standards](https://www.w3.org/TR/WCAG21/) of accessibility across global markets through a range of electronic devices including mobiles, tablets, laptops and desktops. It will need to be compatible with a variety of internet browsers, mobile and tablet devices globally. Governments often use outdated browsers and this will need to be accounted for.

## The platform must support a wide global user base across a large variety of languages, cultures and geographical regions, many of whom will have English as a second language. It must, therefore, support frictionless translation into a number of languages (most importantly French, Spanish, Arabic).

## The platform must also offer a simple and intuitive user journey, in order to be accessible to different cultural audiences and across different languages, taking into account all levels of digital skills and experience.

## **Design and iteration**

### The Supplier should have strong visual design capability, specifically UX capability

### The Supplier will have an iterative, test-and-learn approach to design and production and experience in designing to meet user needs.

## **Reporting and evaluation**

### Based on this evaluation, the Supplier will work closely with CO to improve user engagement as required.

## **Working with the GCS Product Team**

## The Supplier will have a flexible approach to working with CO, with an openness to co-creation.

## The Supplier will agree on the team members allocated to the project. The GCSI Product Team expect to use a "One Team" approach to delivery, with supplier development staff also available to the CO Team for communications.

### The Supplier will allow the CO Team to interact directly with all staff working on the project.

### The Supplier will use the tools and processes for delivery as agreed with GCSI.

# key milestones and Deliverables

## The following Contract milestones/deliverables shall apply:

|  |  |  |
| --- | --- | --- |
| **MILESTONE / DELIVERABLE** | **DESCRIPTION** | **Timeframe or DELIVERY DATE** |
| Project kick-off | Identify initial priorities of the requirement, agree approach and establish ways of working | Within 2 weeks of award date |
| Hosting cutover | Perform necessary steps to establish hosting ownership of platform and agree development roadmap | Within 2 weeks of award date |
| Soft launch  | Snagging issues to be resolved | Within 1 month of award date |
| Project live | Reach definition of success as defined in kick-off phase. Agree roadmaps for future projects. | Within 6 weeks of award date |

#

# MANAGEMENT INFORMATION/reporting

## The Supplier will report to a named day-to-day CO lead.

## A project delivery team drawn from CO and including the project manager and team as needed from the Supplier will meet regularly, at least once a week, including frequent face-to-face/video call working sessions, Covid restrictions permitting.

# volumes

* 1. The platform will be available to a global audience of government communicators between 1 - 5,000 users annually.

# continuous improvement

## The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

## The Supplier should present new ways of working to the Authority during annual Contract review meetings.

## The Supplier and GCSI will work in accordance with the principles of Agile development. The Supplier will have an iterative, test-and-learn approach to design and production and a knowledge of how to design to meet user needs.

## The courses will be continuously improved in line with user feedback and developments in industry best practice.

## Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.

# Sustainability

* 1. Products should be developed with due regard to environmental impact, diversity and equality within the [UK sustainability goals](https://www.gov.uk/government/publications/implementing-the-sustainable-development-goals/implementing-the-sustainable-development-goals--2).

# quality

## The Supplier will adhere to Digital Learning standards and Accessibility guidelines outlined in the [GDS Service Manual.](https://www.gov.uk/service-manual)

## The Supplier will adhere to user requirements as identified in any user testing by CO.

## The Supplier will adhere to style guidelines as supplied by CO.

## All content is to be approved by CO before being released.

## The technical platform must facilitate the moderation of user-generated content (e.g. discussion boards) by CO at a local and global level.

# PRICE

## The Supplier will provide the total price of the contract to meet the requirement.

## In addition, the price should be broken down as appropriate into the following components:

### Annual hosting cost (including installation and set-up, server cost)

* + 1. Annual maintenance cost (including support coverage)
		2. Development cost (day rate to cover adequate development budget)

 Further details on pricing can be found in Attachment 4.

# STAFF AND CUSTOMER SERVICE

## The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

## The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

## The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

# service levels and performance

## The Authority will measure the quality of the Supplier’s delivery by:

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Meeting production timeframe | Key production milestones to be achieved in the timeframes stated in 7.1 | 100% |
| 2  | Quality | Technical development projects completed to an excellent standard as measured by internal stakeholder and user feedback  | 95% |
| 3 | Staffing | Supplier sufficiently staffed to meet GCS needs through contract duration  | 100% |
| 4  | Security Needs | Supplier meets security requirements as stated in 16 | 100% |
| 5 | Support | Support SLAs as outlined in 6.2 to be sufficiently met  | 100% |
| 6 | Project Meetings | A project delivery team drawn from GCSI and including the project manager and team as needed from the Supplier, will meet regularly, at least once a week,  |  |
| 7 | Performance Review Meeting | The Parties shall attend meetings to discuss Performance Monitoring Reports on a Monthly basis. |  |

## Should the Supplier fail to meet any Service Level Performance Measure the Buyer reserves the rights to terminate the Contract early in accordance with the terms and conditions.

## The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

# Security and CONFIDENTIALITY requirements

## Suppliers must have appropriate and documented IT, physical, personnel and procedural security measures in place to prevent any unauthorised access to, or leakage of, data collected as part of the training, and to prevent it being shared with any unauthorised third parties.

## **Certification Requirements**

### The Supplier must have a current and valid Cyber Essentials Plus Certificate awarded by one of the Government approved Cyber Essentials accreditation bodies within the last 12 months (see: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview) and/or a current and valid ISO 27001:2013 Certification, or be willing to obtain one of these certifications within three months of contract award.

## **Patching and Penetration Testing/IT Health Checks**

### The Supplier must proactively monitor Supplier vulnerability websites and demonstrate the ability to ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the Cloud Security Principles https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

### The Supplier must undertake the following security assurance activities at their own cost and expense to demonstrate that the people, processes, technical and physical controls have been delivered in an effective way:

#### Penetration testing to be carried out by certified CREST or CHECK supplier, within 3 months of Contract Award.

#### Penetration testing of the production environment must be done before any Authority data is stored or processed on the platform,

#### The penetration testing scope must include any devices used to manage the solution,

#### An annual penetration test must be undertaken with the scope agreed with the Authority and when there is a significant change to the infrastructure/service,

#### After receiving the penetration testing report, the full report must be shared with the Authority and the Supplier must produce a remediation plan to agreed timescales which must be agreed with the Authority.

## **Physical Security**

### On physical security, the Supplier must have appropriate physical security measures in place in any data centres used to host the Authority’s data and should describe in detail what those measures are.

## **Personnel Security**

### Potential bidders will ensure before the contract term begins that all staff have undergone pre-employment checks to a minimum of the Government Baseline Personnel Security Standard.

## **Risk Management Documentation**

### The successful Supplier will prepare a Risk Management Document (a template will be provided by the Authority), which details the information assurance and security controls applied to the delivery of the solution. This will include how the Supplier is meeting the Cloud Security Principles: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

### The Supplier will need to keep this document updated to reflect the current security position at least annually during the life of the contract.

## **Protective Monitoring**

### The Supplier must ensure that they have a protective monitoring solution and regime in place at all times and must be able to provide evidence of such.

## **General Data Protection Regulation (GDPR) Compliance**

### Full compliance with the GDPR and any other applicable data protection laws is essential, with the Authority being the Data Controller and the Supplier being the Data Processor.

## **Hosting**

### The course will ideally be hosted in the United Kingdom. In order to meet current GDPR requirements, the solution must be hosted within the European Economic Area (EEA) or have equivalent measures in place (e.g. Privacy Shield or model contract clauses)

## **Third Party Suppliers**

### Any Third-Party Suppliers involved in the delivery of the solution must meet with the certification requirements at 17.1.1 unless agreed otherwise by the authority.

## **Incident Reporting**

### Any security incidents relevant to the solution must be reported to an agreed point of contact within the Authority within two working days.

# payment AND INVOICING

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

## Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

## Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

## Invoices should be submitted to: hannah.harrison@cabinetoffice.gov.uk

# CONTRACT MANAGEMENT

## Attendance at Contract Review meetings shall be at the Supplier’s own expense.

# Location

* 1. The location of the Services will be carried out on-line, and by the Authority within Government offices in Whitehall, London, UK.