Crown Commercial Service

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

CONTENTS

1. PURPOSE

1.1 The Government Communication Service (GCS) requires an external Supplier to provide a digital learning delivery platform or learning management system.

1.2 The Supplier will support the delivery of our GCS Advance Programme by providing a dedicated cloud-based Learning Management System (LMS) instance that allows us to offer our users a seamless service whilst maintaining robust security and data protection.

1.3 The Supplier will support integrations between the LMS instance and other government platforms designed to improve management of the Advance programme and scaling of digital learning courses to new markets.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Cabinet Office is the centre of the UK Government. Its purpose is to: support the Prime Minister and Cabinet to deliver the Government's programme; drive efficiencies and reforms that will make Government work better; create a more united democracy; and strengthen and secure the United Kingdom at home and abroad.

2.2 GCS is the professional body for people working in communication roles across Government. Its aim is to deliver world-class communications that support Ministers' priorities, improve people's lives and enable the effective operation of our public service. It serves both politicians and the public alike.

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 GCS has been building its digital learning capability over the last few years. To deliver digital learning effectively at scale and improve the service to our learners via more personalisation, flexibility and functionality, GCS must be able to offer courses online via a high quality digital platform. To maintain the service to users we need support in maintaining and integrating the LMS instance and related components that make up our learning platform.

3.2 A focus has been placed on deepening integrations between the LMS and the GCS platform for member services, GCS Connect. Integrations include ensuring Single Sign On (SSO) via Open ID Connect between the two platforms is maintained.

3.3 The service is expected to see an average annual usage of approximately 6,000 users.

4. DEFINITIONS

Expression or Acronym	Definition
SaS	Skills and Standards
GCS	Government Communication Service
Govt Skills	Government Skills Unit
GCS Connect	The membership platform which will house user data and allow learners to display their learner record.
GCS Advance	Is the new L&D programme for Government Communication Service members in the UK public sector.
Practitioner	The digital learning led L&D offer of GCS Advance.
Leader	The in person offer for senior leaders
Expert	The in person offer for managers and deep discipline experts
EdX	The learning platform currently used by GCS.
CO	Cabinet Office or the Contracting Authority
LMS	Learning Management System
CDIO	Central Digital and Information Office within Cabinet Office

5. SCOPE OF REQUIREMENT

5.1 GCS requires a Supplier to provide continuous hosting for our cloud-based digital learning platform and support with any interruptions of live service.

5.2 GCS will require bidders to provide a summary of their proposed platform solution, as well as details of their experience working with learning platforms in other comparable learning contexts.

5.3 The Supplier should include a portfolio of credentials outlining their evidence of past project delivery in this field within their tender proposals.

5.4 The learning platform can store and manage all GCS training material giving us a centralised location across GCS where our learners can get instant access and find the support they need.

5.5 The LMS must support easy discoverability of learning, blended learning, instructor-led virtual training, gamification, leaderboards, customisable pages, forums & comments, skill gap management, shared learning repository.

5.6 The LMS must support training materials including various formats such as SCORM, videos, and documents along with live webinars and virtual instructor-led training.

5.7 Course management features must include creating different cohorts or course runs, capping enrolments, tracking attendance, and automating enrolments onto selected course runs.

5.8 The LMS must support manual addition of learning records such as previous CPD points.

5.9 The LMS must provide robust reporting features that allow us to measure learning effectiveness.

5.10 The LMS must be customisable and to some extent brandable to fit with the GCS brand guidelines.

5.11 The LMS must provide easy management information dashboards to showcase which teams are using and completing their learning.

5.12 The LMS must offer tailored learning experiences with different learning pathways based on their experience, seniority and previous course choices and personalised dashboards.

6. THE REQUIREMENT

6.1 Billing

6.1.1 The Supplier shall provide a yearly invoice and a quarterly usage report.

6.2 Collaboration

6.2.1 The Supplier must be able to work with CO stakeholders for the purposes of integrating with other government platforms.

6.2.2 During onboarding, the Supplier shall allocate team members to the project as needed. The GCS SaS Team expects to use supplier staff available to the CO Team upon request.

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

6.2.4 The Supplier shall work with the GCS SaS Team to support the readiness of the LMS for the delivery of a Practitioner Programme in October 2025 and beyond.

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

6.3 Documentation

6.3.1 The Supplier should provide comprehensive documentation, including user manuals, system architecture, API documentation, and any other relevant technical documentation, so that the SaS team are able to 'self manage' the LMS on a day to day basis.

6.4 Integration

6.4.1 The LMS must be able to handle integration across multiple fields (name, email etc) and be flexible in adding new fields as needed.

6.4.2 The LMS must assure integration between data held in GCS Connect or Govt Skills platforms, including the forthcoming Government Campus, with the intention of simplifying the learner registration process.

6.4.3 The LMS should allow Learners to receive notifications and updates regarding course enrolments, deadlines, announcements, and any changes to the course content.

6.4.4 The LMS should allow the front end (landing page) to enable learners to enrol on courses directly from the front-end interface.

6.4.5 The LMS must provide a functioning data dashboard for GCS team to interpret and gain insights.

6.4.6 The LMS should allow Administrators to have access to customisable reports and analytics dashboards for monitoring the performance and effectiveness of the integrated learning portals.

6.4.7 The LMS will allow integration with existing CO and Supplier Systems (such as GCS Connect, Government Skills Campus), using standard protocols or APIs to enable a seamless user experience.

6.5 Maintenance

6.5.1 The Supplier will be responsible for providing customer support for the LMS according to mutually agreed SLAs.

6.5.2 The Supplier should provide ongoing technical support, bug fixes, and regular updates for the LMS, ensuring its smooth operation and compatibility with future changes in the integrated learning portals.

6.5.3 When available, the Supplier schedule will ensure the LMS receives periodic and timely software upgrades.

6.6 Scalability

6.6.1 The Supplier shall ensure that the LMS is scalable and able to handle approximately 20,000 learners and up to 6,000 concurrent user sessions without compromising performance.

6.6.2 The Supplier will setup new LMS environments as required by GCS to provide either testing environments or the means to ensure courses are available to multiple audiences.

6.7 Security

6.7.1 The Supplier shall ensure that the LMS will adhere to GCS and CDIO data privacy regulations, such as GDPR, ensuring user consent and the handling of personal data.

6.7.2 The Supplier shall ensure that the LMS will adhere to GCS and CDIO security practices to protect user data, including encryption of sensitive information and secure transmission of data between the front end and back-end systems.

6.8 Technical Capability

6.8.1 The Supplier will demonstrate technical capability sufficient to maintain and improve its learning platform.

6.8.2 The learning platform can store and manage all our training material giving us a centralised location across GCS where our learners can get instant access and find the support they need.

6.8.3 The LMS must support easy discoverability of learning, blended learning, instructor-led virtual training, gamification, leaderboards, customisable pages, forums & comments, skill gap management, shared learning repository.

6.8.4 The LMS must support training materials including various formats such as SCORM, videos, and documents along with live webinars and virtual instructor-led training.

6.8.5 Course management features must include creating different cohorts or course runs, capping enrolments, tracking attendance, and automating enrolments onto selected course runs.

6.8.6 The LMS must support manual addition of learning records such as previous CPD points.

6.8.7 The LMS must provide robust reporting features that allow us to measure learning effectiveness.

6.8.8 The LMS must be customisable and to some extent brandable to fit with the GCS brand guidelines.

6.8.9 The LMS must provide easy management information dashboards to showcase which teams are using and completing their learning.

6.8.10 The LMS must offer tailored learning experiences with different learning pathways based on their experience, seniority and previous course choices and personalised dashboards.

6.9 Accessibility

6.9.1 The Supplier will ensure the platform offers a simple and intuitive user journey, in order to be accessible to different cultural audiences and across different languages, considering all levels of digital skills and experience.

6.9.2 The Supplier will ensure the platform supports industry and WCAG 2.2 standards 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.

7. KEY MILESTONES AND DELIVERABLES

7.1 The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Timeframe or Delivery Date
Creation of cloud based instance of LMS for GCS	October 2025
Complete customisation and onboarding of LMS platform, including SSO integration with other GCS platforms	End of October 2025
Further customisation of the platform	End of Q3 (December) 2025
Launch GCS Advance practitioner cohort registrations	March 2026
Launch GCS Advance Expert and Leader cohort registrations	May 2026

Maintain live service reliability, troubleshoot communicate any periodic updates or interruptions of service well in advance	Throughout

8. MANAGEMENT INFORMATION/REPORTING

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

9. SUSTAINABILITY

9.1 Products should be developed with due regard to environmental impact, diversity and equality within the UK sustainability goals.

10. QUALITY

10.1 The Supplier will adhere to Digital Learning standards and Accessibility guidelines outlined in the GDS Service Manual.

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

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

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

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

11. PRICE

11.1 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

11.2 The Supplier will provide the total price of the contract to meet the requirement of 6,000 users per year.

12. STAFF AND CUSTOMER SERVICE

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

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

12.3 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.

13. SECURITY AND CONFIDENTIALITY REQUIREMENTS

13.1 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 and to prevent it being shared with any unauthorised third parties.

13.2 Certification Requirements

13.2.1 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.

13.3 Patching and Penetration Testing/IT Health Checks

13.3.1 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

13.3.2 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.

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

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

13.3.5 The penetration testing scope must include any devices used to manage the solution.

13.3.6 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,

13.3.7 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.

13.4 Physical Security

13.4.1 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.

13.5 Personnel Security

13.5.1 Potential Providers will ensure all staff have undergone pre-employment checks to a minimum of the Government Baseline Personnel Security Standard (or equivalent).

13.6 Risk Management Documentation

13.6.1 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

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

13.7 Protective Monitoring

13.7.1 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.

13.8 General Data Protection Regulation (GDPR) Compliance

13.8.1 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.

13.9 Third Party Suppliers

13.9.1 Any Third Party Suppliers involved in the delivery of the solution must meet with the certification requirements at 15.1 unless agreed otherwise by the authority.

13.10 Incident Reporting

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

14. PAYMENT AND INVOICING

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

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

14.3 Invoices should be submitted to: TBC AT AWARD

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