**Call-Off Schedule 20 (Call-Off Specification)**



**Statement of Requirements**

Provision of Corporate Web Access

Contract Reference: CCTS24A41

**CONTENTS**

[1.](#_heading=h.45tzjsaec47u) PURPOSE 3

[2.](#_heading=h.b5apo16e514r) BACKGROUND TO THE Buyer 3

[3.](#_heading=h.93cysdxlsfkp) Background to requirement/OVERVIEW of requirement 3

[4.](#_heading=h.6y4d8w1l6ka0) definitions 4

[5.](#_heading=h.vz4y7s5538ff) scope of requirement 5

[6.](#_heading=h.mdvogxmjew1i) The requirement 6

[7.](#_heading=h.j5yd3l2xb8p4) key milestones and Deliverables 11

[8.](#_heading=h.lnxbz9) MANAGEMENT INFORMATION/reporting 12

[9.](#_heading=h.3q84ejf859j1) volumes 15

[10.](#_heading=h.b2x0y16c8bok) continuous improvement 15

[11.](#_heading=h.ufnwt1e7020u) Sustainability / SOCIAL VALUE 16

[12.](#_heading=h.fhtxz5xdmdcz) quality 16

[13.](#_heading=h.86vvnchcspnw) PRICE 16

[14.](#_heading=h.kj3kp92ysdts) STAFF AND CUSTOMER SERVICE 16

[15.](#_heading=h.ikyezn6ch5nl) service levels and performance 17

[16.](#_heading=h.2xcytpi) Security and CONFIDENTIALITY requirements 17

[17.](#_heading=h.g6o4k26k6n5t) payment AND INVOICING 18

[18.](#_heading=h.gaafm8cxqkjq) CONTRACT MANAGEMENT 18

[19.](#_heading=h.3iqcti7um0m9) Location 18

# PURPOSE

## The purpose of this procurement is to replace Cornwall Council’s current on-premises web access solution, which has increasing operational support overheads and functional issues, with a modern, cloud-based secure web access solution that supports the use of cloud applications, hosted services and better aligns with flexible and remote working practices employed throughout the authority.

# BACKGROUND TO THE Buyer

## Cornwall Council is a local government organisation of over 10000 employees with 8000+ managed client devices (predominantly Microsoft Windows), 4000 mobile devices and 300 public access workstations. These endpoints work from over 150 Wide Area Network (WAN) sites across Cornwall and the Isles of Scilly, as well a significant proportion, approximately 3500 per day, working from home or remote locations.

## The authority’s core web access and content filtering service design has remained largely unchanged for over 15 years, with the only major updates being through lifecycle technology upgrades and associated feature releases.

* 1. The solution is a traditional on-premises data centre Secure Web Gateway (SWG) deployment, scaled/licensed to support 6800 concurrent users, with virtual appliances deployed on the internal corporate (CC) domain and physical appliances deployed on the public access (PN2) domain.
	2. The Council are currently, through lifecycle necessity, in the process of migrating the PN2 domain services onto a cloud-based solution through our existing vendor, Forcepoint. We expect that project to be completed in early 2025.

## The Council has recently completed the migration of all corporate network locations to a new managed WAN with incorporated perimeter firewall services, internet access and cloud connect access gateways (to Azure, AWS, etc) within the supplier network. The new design allows for more direct access to internet services from each network location via a private cloud high-capacity gateway, without the dependency on the Council’s lone on-premises Data Centre, based in Truro, Cornwall.

# Background to requirement/OVERVIEW of requirement

## Cornwall Council’s current secure internet access platform categorises, inspects, and logs web-bound traffic from a diverse range of clients operating in various physical locations. These include fully managed corporate devices running Microsoft Windows assigned to individual officers, shared devices used by citizens in Cornwall Council-supported spaces, and infrastructure devices performing Internet of Things (IoT) activities. The current internet access services are provided through a hybrid Forcepoint solution which is majority hosted on-premises, with a limited cloud presence for the Public Access Network and unauthenticated traffic. The solution is scaled for a total of 6800 user licenses, with 6500 Corporate users routing via Forcepoint's traditional Secure Web Gateway product and 300 licenses assigned for Public Access on the Forcepoint ONE cloud platform. All corporate internet-bound traffic, except some approved cloud service destinations such as Microsoft M365, route through the corporate network to reach proxy services and then subsequently route outbound via the Council's centralised on-premises primary internet connection.

## Proxy bypass exceptions and “local breakout” for corporate users and services are managed and maintained by operational teams through a combination of WPAD exceptions, multiple infrastructure firewalls and client firewall policy. The demand for exceptions has significantly increased over recent years, as the demand for cloud-based applications and hosted services has grown.

## The current SWG design is inefficient and does not exploit the benefits of our new WAN infrastructure. The solution has ever increasing operational support overheads, suffers from functional issues as we continue to mature with our use of cloud applications and hosted services and, significantly, the current solution does not support mobile devices.

## The following diagram represents, at a high level, the complexity of internet access as currently deployed.

## A diagram showing multiple web filtering products in use for different user personas within Cornwall Council.  The diagram highlights the complexity of the infrastructure as currently deployed.

## Cornwall Council is seeking to replace its existing on-premises secure internet access platform with a modern, cloud-based solution. This new solution must deliver secure web access that supports our officers in their work for the citizens of Cornwall. The initial requirement of this procurement is to ensure a seamless transition from the current system to a new, more efficient, and secure platform.

## In addition to replacing the existing system, Cornwall Council aims to develop a strategic partnership with the chosen supplier to move towards a zero-trust security model. This strategic direction is driven by the decentralization of our workforce and the retirement of on-premises hosted systems in favour of SaaS platforms, in line with industry trends. The planned closure of our remaining data centre in 2030 will further drive the adoption of SaaS products to replace legacy systems. While this procurement does not directly encompass these components, the chosen secure internet access solution will represent the first step in this process and must support integration into a broader SASE cloud security architecture, embracing continuous verification and dynamic risk-based policy postures.

# definitions

|  |  |
| --- | --- |
| **Expression or Acronym** | **Definition** |
| Public Access (PN2) | means a network dedicated to the provision of publicly accessible internet access to users of managed computers within Cornwall Council buildings. |
| Corporate VPN | means Virtual Private Network – a secure network connection established by trusted remote clients, terminated within the on-premises infrastructure of Cornwall Council. |
| Internal corporate (CC) domain | means the main administrative boundary within which all Council Staff accounts and almost all computer objects are located. |
| DMZ | means demilitarized zone -- a perimeter network that protects the internal local-area network from untrusted traffic |
| WPAD | means Web Proxy Auto-Discovery Protocol |
| SaaS | means Software as a Service |
| SASE | means Secure Access Service Edge |
| CASB | means Cloud Access Security Broker |
| SIEM | means Security Information and Event Management |
| ITSM | means Information Technology Service Management |

# scope of requirement

### The following are core requirements to any solution:

### To supply and implement a cloud based secure internet access solution that meets the technical & functional requirements defined in this Statement of Requirements.

### The successful vendor will supply, install, test and bring into operational readiness all agreed elements of the proposed solution, including any hardware, software or client applications which may be necessary to meet the requirements defined in this Statement of Requirements.

## Integration of the new solution with existing infrastructure.

## Successful transition of all existing CC web access workloads (Corporate Domain, Public Access, Councillor WiFi) from the current Secure Web Gateway solution.

## No internet traffic to traverse the corporate client VPN, except where explicitly desired.

## Full migration of Corporate and Public Access domain services to the new solution.

## Managing the implementation of the solution so that full migration of in-scope domain services is achieved.

# The requirement

## The proposed solution must meet the below mentioned technical & functional requirements and design objectives.

## General

## The supplier must provide a comprehensive cloud based secure web access solution where all identified user and device domains included within the scope of works are successfully migrated onto the new solution in line with the outline delivery milestones identified in Section 7.

## The solution must be a dedicated secure internet access solution that provides common Secure Web Gateway features like Web Proxy, web content filtering, URL filtering, Antivirus, Anti-malware, Application visibility & control, SSL inspection, protocol filtering, detailed logging, reporting and management.

## The solution must be a cloud-based platform, delivered as SaaS.

## Any connectivity required between the cloud service and Cornwall Councils infrastructure (i.e. IPSec VPN, GRE tunnel, etc) must be compatible with existing firewalls.

## The solution must support a total of 7800 concurrent managed users at the point of delivery and be scalable to support 25% growth over 5 years.

## Notifications must be provided to Cornwall Council for any updates to components within the scope of the solution.

## The supplier must be able to provide operational support for the solution within UK working hours of Monday to Friday from 8am to 6pm (excluding Bank Holidays).

## The supplier must provide service level(s) that meet a target SLA response for Priority 1 faults within 30 minutes and Priority 2 faults within 60 minutes.

## The Supplier must ensure that the Authority receives email updates and notifications for raised support calls.

## The solutions cloud service availability must meet or exceed 99.99% available.

## Web Content Filtering, Inspection and Policy

## The solution must have inbuilt URL filtering functionality with multiple pre-defined categories. It must support the creation of custom URL categories for allowing/blocking specific domains/destinations as required by the organisation.

## All web browsing traffic must be subject to a categorisation process, supported by a policy engine to block / permit access as required. This must include capabilities to support exceptions for specific endpoints, identities or non-standard web ports.

## The solution must have a strong content filtering database with URLs segregated into different groups/categories, which should be automatically updated with latest changes on a regular basis.

## The solution must provide predefined categories to allow the easy blocking of illegal and undesirable content. Re-categorisation of sites between categories must be possible, as well as the creation of custom categories.

## The solution must support the ability to create exceptions to category filters by category, source IP/hostname/username and destination URL/IP/FQDN.

## The solution must be able to prevent users from exposure to potentially unsafe content not already blocked via categorisation.

## The solution must have the option to enforce content, application, hash value, key word/regular expression and protocol based blocking.

## The solution must be able to provide a safe search URL option or otherwise be able to filter search engine results (including images).

## The solution must have web protection mechanism(s) to identify and block web pages that have malicious scripting or executable code.

## The solution must have the option to allow or deny a particular domain or destination for a user or IP group permanently or for a specific time period.

## The solution must support actions for websites/applications such as allow, monitor, block, time-based access, etc.

## The solution must be able to restrict a user/groups access to internet or specific set of URLs/groups/categories/IP address(es) during specified hours, time periods or based on bandwidth quota.

## The solution must be able to perform HTTPS traffic deep packet inspection (SSL/TLS based) to identify threats and data loss in encrypted traffic.

## The solution must allow customisation that supports branding of presented content to end users – i.e informing of the reason a web request is blocked.

## The solution must provide mechanisms for user self-service risk acceptance when accessing higher risk sites (i.e. ‘web collaboration’ category or to specific destinations) and be auditable.

## The solution must allow embedded HTTPS links within responses to end users – i.e links to a service management tool.

## The solution must be able to scan real time downloads and show the status page to end user. In cases where infections are found, it should restrict the user being able to download the file.

## The solution must provide capabilities that allow endpoints whose architecture or configuration mean that they are unable to pass credentials to utilise secure web browsing services.

## The solution must be able to handle Web 2.0 technologies, such as Web Sockets, without the need for additional configuration or exceptions.

## The solution must offer the ability to bypass SSL/TLS inspection for specific source or destinations.

## The solution must provide the capability to restore to a known good configuration state.

## The solution must offer the ability to set a fixed source IP address or IP Range for outbound connections from the Council’s environment.

## Cyber Security

## The solution must provide advanced threat prevention against cyber-attacks like malware, ransomware, supply chain attacks and phishing.

## The solution must utilise the global threat intelligence network to protect from Zero day attack, blended threats, Botnet, Trojan, Malware communication, Spyware, Pharming attack and traffic - including compressed files.

## The solution must be able to block, allow or monitor only using Anti-Virus signatures.

## The solution must prevent data loss by making sure that enclosures or disks removed after maintenance, failure, or misappropriation are kept secure and the data remains inaccessible.

## The solution must be able to encrypt storage, as required, when at rest.

## The solution must include role-based administration.

## The data migration process for all workloads must have no or minimal operational impact to existing configured hosts or servers.

## Suppliers must hold a valid NCSC Cyber Essentials certification, with a preference for Cyber Essentials Plus certification. This ensures that appropriate cyber security controls are in place to protect against common cyber threats and to demonstrate a commitment to maintaining high standards of cyber security.

## The solution must be Data Protection Act 2018 and UK GDPR compliant.

## Logging and Reporting

## Logs showing user activity must be retained for a minimum of 90 days.

## Logs of user activity must contain sufficient detail to comprehensively and unambiguously identify the user and the destination endpoint being accessed.

## A notification system must exist to alert Cornwall Council to any changes in the state of the solution provided either in advance of planned works or in the event of unplanned state changes.

## The solution must provide the capability to report on bandwidth utilisation based on source, endpoint or destination site both on WAN and remote connections.

## The solution must be capable of providing security events to a 3rd party managed SIEM solution.

## Reports that are generated based upon reporting data, must be secured with tamper proofing mechanisms guaranteeing the integrity of their output.

## The generation of reports must not adversely affect the operation of the policy enforcement or any other end user experience of the system.

## The solution must alert based on intrusion detection and device removal alerts.

## Management and Client

## The solution must include the ability to view an audit log of administrator actions.

## The solution must support OpenID or SAML2 Single Sign-On (SSO) using Microsoft EntraID for logons to administrative and reporting portals.

## The solution must support multifactor authentication for logons to administrative and reporting portals.

## Any internet accessible management portals must use HTTPS, secured by a minimum of an externally signed and trusted SHA256 certificate.

## The solution must support the use of Microsoft EntraID, Hybrid Entra ID with Active Directory and standalone on premises Microsoft Active Directory as identity providers.

## The solution must provide the capability to handle user data according to different privacy and data processing commitments. For example, data held through the use of public internet access should be separated from data held through corporate internet access.

## The solution must support role-based access control for administrator accounts – i.e. allowing reporting only access.

## The solution must support multi-user environments, such as Citrix and Azure Virtual Desktop.

## The solution must be compatible with the following user agent operating systems, including long term servicing channel versions: Window 10/11, Apple macOS, Android, iOS, Linux, Azure Virtual Desktop and Windows 365 clients.

## The solution must be compatible with managed endpoints that use Microsoft Defender endpoint protection and response software.

## The solution must support silent deployment via Microsoft InTune and Microsoft SCCM.

## Delivery Approach

## The Supplier must be accountable for technical leadership and managing and delivering the entire solution to agreed timescales, even if partners or third parties are involved.

## The Supplier should develop and provide a suitable delivery artefact that ensures all parties understand and agree on the scope, expectations, deliverables, milestones, control and management of the solution's delivery to Cornwall Council.

## The Supplier must provide a design document, to an agreed standard, describing how the solution interacts and functions with Cornwall Council’s technical environment. The Supplier must confirm if there is an additional cost for this design document and itemise the cost in their response.

## The Supplier must provide and manage a suitable delivery plan tailored for Cornwall Council’s solution scope so that all parties have a mutually agreed upon, clear understanding of delivery expectations and timelines. This plan should identify key stages, deliverables, milestones, activities, artefacts, dependencies, and necessary delivery resources. The timelines should be realistic for an organisation of Cornwall Council’s type and scale.

## The Supplier’s resources, partners, and third parties must work during Cornwall Council's hours and be available for out-of-hours work when needed. The Supplier must confirm any additional costs for out-of-hours work and provide a rate card.

## The Supplier must track and control use of their delivery resource days and report and manage any risks of exceeding the forecast. They must confirm if any additional resource costs may be incurred and provide a rate card

## To keep all team members from the Supplier and Cornwall Council informed and aligned, the Supplier should hold regular progress meetings and share the delivery controls they will use to manage the solution's delivery, such as:

## a managed log of risks, issues, actions, decisions, change requests, and lessons learned during the delivery.

## regular progress reports which may include RAG status, progress, resource burn-down, and any delivery alerts.

## a regularly updated itemised register of goods and services, including details of their delivery, installation, and operational status.

## Whether as part of the project scope document, or some other delivery artefact, the Supplier should describe their approach to providing initial support, troubleshooting, and configuration adjustments during the transition to full acceptance into service. The Supplier should also describe their approach to managing the risk of integration issues with the existing infrastructure and providing support in resolving any impacts.

## The Supplier should deliver a pilot as part of the transition. The Supplier should confirm the number of use cases and users supported, the duration of the pilot, the level of support, and explain what happens after the pilot concludes.

## The Supplier should provide guidance to Cornwall Council staff on how to quality assure, or test, the solution before go-live.

## The Supplier should provide training or knowledge transfer to ensure a minimum of four Cornwall Council IT staff receive the necessary skills, at the appropriate times, to operate and maintain service.

# key milestones and Deliverables

## The following Contract milestones/deliverables shall apply:

|  |  |  |
| --- | --- | --- |
| **Milestone/Deliverable** | **Description** | **Timeframe or Delivery Date** |
| 1 | Ready to begin delivery* Supplier delivery/implementation resources named
* Project initiated
* Initial discovery/planning/design workshop
 | Within 1 month of Contract Award |
| 2 | Full migration of all in-scope domains and workloads to new platform  | No later than 1st February 2026 |

# MANAGEMENT INFORMATION/reporting

## Contract Management

## Contract Review Meetings:

## The Supplier shall attend a quarterly service review meeting on-site at the Authority’s premises located at Truro, Cornwall where practicable, or via Teams conference.

## On an annual basis, the meeting will be expanded to enable a more strategic annual review. This will focus on reviewing the previous year’s successes, and forward planning for the coming year, taking into account market trends, road mapping, and continuous improvements.

## Proposed Terms of Reference, including outline agendas are included in Annex A to Call-Off Schedule 15 (Contract Management), the Council welcomes your views and feedback on these.

## Performance Management:

## The Supplier shall establish processes to monitor its performance against the agreed KPIs / PIs.

## The Authority shall review progress against these KPIs to evaluate the effectiveness and efficiency of which the Supplier performs its obligations.

## An indicative template which provides details of performance indicator requirements is included within Annex B to Call-Off Schedule 14 (Service Levels) and the Council requests the Bidder proposals in relation to targeted performance management and reporting.

## Suppliers are requested to submit example performance reports as part of their response.

## The final Key / Performance Indicators will be jointly developed and agreed within the first 3 months of service commencement. This will include agreement on performance target levels, reporting processes, breach tolerances, and applicable service credits.

## Management Information:

## The Bidder shall supply Management Information (MI) reports to the Authority each month.

## The Supplier must provide comprehensive reports, and reporting tools to allow the Customer to fully understand their use of the Services on a monthly (or quarterly basis if required by the Customer) capable of being exported from the Call Off Commencement Date into Excel at no additional cost ideally accessible via an online portal.

## The MI reports are to contain the following information as a minimal:

## Key deliverables / activities in this period.

## Key deliverables / activities planned next period.

## Details of any service requests not resolved within agreed SLA, and associated credit applications.

## Details of any service incidents not resolved within agreed SLA, and associated credit applications.

## Service Usage reporting – including zero usage, high utilisation.

## Capacity management.

## Suppliers are requested to submit example management information reports as part of their response; along with details regarding proactive MI reporting and analysis.

## Service Level Management

## The bidder shall provide details of your proposed Service Desk. Responses should include details of:

## The operating hours and locations of the Service Desk

## The options for contacting the Service Desk (eg. by phone, email, online, etc.)

## How calls are answered, including SLA on time to answer

## The approach to dealing with service incidents and problem resolution, including:

## Prioritisation and classification by level of severity

## Incident management processes

## Incident detection and recording processes

## Incident monitoring, tracking, and communication processes

## Resolution and closure processes, including Council approval requirements

## Escalation procedures when dealing with service incidents, including an organisational chart showing the personnel involved in the escalation process

## Methods available to enable the Council to monitor call status and progress (eg. web portal access)

## Council responsibilities when interfacing with the Service Desk

## Please provide details of your proposed service levels for the solution. The response should include details of:

## The MTBF level(s) associated with their solution

## How availability levels are defined, measured, and monitored

## How service incidents are defined

## The service restoration times offered

## How your proposed service levels underpin the Council’s internal service levels as detailed in Call Off Schedule 14 – Service Levels.

##

# volumes

## Current contract spend in Secure Web Gateway services is £60k per annum and scaled to support 6800 concurrent connections/users – split by environment as follows:

## Corporate Domain (CC) – 6500 licenses

## Public Access Domain (PN & DMZ) – 300 licenses

## Cornwall Council supports the use of approximately:

## 8000 windows devices on the corporate domain

## 550 physical and virtual servers

## 300 workstations on the public access domain

## 3000 managed Android mobile devices

## 1000 managed Apple mobile devices.

# 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 Buyer during quarterly Contract review meetings.

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

# Sustainability / SOCIAL VALUE

## The Supplier should meet the social value commitment by ensuring measures are made to deliver one of the following environmental benefits through the delivery of the Contract:

## Tackling climate change.

## Working towards net zero emissions.

# quality

* 1. The Supplier must provide and manage a detailed delivery plan tailored for Cornwall Council’s solution scope so that all parties have a mutually agreed upon, clear understanding of delivery expectations and timelines. This plan should identify key stages, deliverables, milestones, activities, artefacts, dependencies, and the necessary delivery resources.

## If any transition activities are undertaken by the Supplier, then Cornwall Council expects the Supplier to carry out this work with minimal disruption to existing infrastructure and internet access services, respectful of Cornwall Council’s internal Change Control processes.

## The Supplier will provide cloud based secure internet access services for all identified user and device domains included within the scope of works.

# PRICE

## 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.

# 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 Buyer’s vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.

# service levels and performance

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

## Monitoring and evaluating the effectiveness with which the Supplier performs their obligations to fulfil the Contract through a suite of KPIs and SLAs. Further details are shown in Order Schedule 14 – Service Levels.

| **Service Levels** | **Service Credit for each Service Period** |  |
| --- | --- | --- |
| **Service Level Performance Criterion** | **Key Indicator** | **Service Level Performance Measure** | **Service Level Threshold** | **Publishable KPI** |
| Migration of all in-scope Domain services | Completion of Milestones on Migration Plan(target for completion 01/02/26) | 95% | 95% | 0.5% Service Credit gained for each percentage under the specified Service Level  | No |
| Monthly Management / Progress reporting | MI report being delivered to the Contract Manager within 7 days following month end.12x MI reports expected per annum of the Contract.Measurement Frequency - Annual  | 90% | 90% | n/a   | No |
| Response to Service RequestSeverity 1  Critical Fault / Failure  Core Service or \*Key Business Application Total failure (or critically impaired) regardless of the number of users | Measurement Frequency - Quarterly Initial Response 30 minsUpdate frequency every 1 hr | 98% | 98% | 0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure | No |
| Response to Service RequestSeverity 2  Multiple Users impacted by a partially non-functioning or inaccessible Core Service or Key Business Application/s (irrespective of root cause) when no other access route is available | Measurement Frequency - Quarterly Initial Response 1 hourUpdate frequency 2 hr update | 95% | 95% | 0.2% Service Credit gained for each percentage under the specified Service Level Performance Measure | No |
| Response to Service RequestSeverity 3  Minor Impact Faults   | Measurement Frequency - Quarterly Initial Response 3 hrUpdate frequency 8 hr update  | 92% | 92% | n/a | No |

# Security and CONFIDENTIALITY requirements

## All personnel involved in the design and implementation work for this project must possess a valid Baseline Personnel Security Standard (BPSS) clearance. This clearance must be obtained and verified prior to the commencement of any project-related activities. The contractor is responsible for ensuring that all staff members meet this requirement and for maintaining records of their clearance status throughout the duration of the project.

## All information related to the requirements of this security product must be treated as confidential and restricted on a need-to-know basis. Access to this information shall be limited to personnel who have been explicitly authorised and have a legitimate need to access it for the performance of their duties. The contractor must implement appropriate measures to ensure that all sensitive information is protected from unauthorised access, disclosure, or misuse.

# payment AND INVOICING

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

## Cornwall Council will issue a call off Purchase Order at Contract award. Any invoices must quote the valid purchase order number in order for payment to be processed.

## 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:

### invoices@cornwall.gov.uk

### Accounts Payable

### Central Scanning Unit

### Unit 17 Threemilestone Ind. Est.

### Truro

### TR4 9LD

# CONTRACT MANAGEMENT

## Contract management details are shown in Order Schedule 15 – Call-off Contract Management.

# Location

## The location of the Services will be carried out at Cornwall Council, County Hall, Treyew Road, Truro, TR1 3AY.