HERTFORDSHIRE COUNTY COUNCIL
STRATEGIC PROCUREMENT GROUP

THE PROVISION OF A MANAGED INTERNET AND WIDE AREA NETWORK INFRASTRUCTURE FOR HERTFORDSHIRE COUNTY COUNCIL CONTRACT REF: HCC0902684

SCHEDULE 1 .2 – SCHOOLS SPECIFICATION

1. INTRODUCTION

In its 1997 consultation paper, "Connecting the Learning Society", the government set out its strategy for funding and building the National Grid for Learning. In Hertfordshire we consulted widely with all of our approximately 550 Local Authority (LA) maintained schools and there was unanimous agreement that we would achieve best value through working together to create a Hertfordshire LA schools local grid for learning and Wide Area Network. After a detailed OJEC procurement process the contract to create this service was awarded to NTL Telewest Business in 1998. We named it the Hertfordshire Grid for Learning (HGfL).

The HGfL was a great success and when we undertook a second OJEC procurement in 2004 the managed services contract was again awarded to NTL: Telewest Business. The contract includes:

- Managed Internet access
- Dedicated service desk and technical resources
- Network services to in excess of 555 schools and Educational sites
- Links to the Council's corporate network and the East of England Regional Broadband Network (E2BN)
- On-line real-time service reporting
- Secure access from the Internet to School networks (VPN)

This second contract will terminate on 31st March 2011.

The HGfL has seen several significant developments over the past 11 years. Whilst some schools were initially connected by 56K dial-up there is now a minimum of 2 Mbps synchronous uncontended broadband linking our primary schools and 10 Mbps at our secondary schools. This has reflected increasing reliance by schools on their connectivity. It started with the Internet providing an interesting way to enhance some lessons but is now absolutely mission critical to all schools not just in their core activity of learning but for every aspect of school life. The HGfL is now equally mission critical to the Council as the delivery mechanism for many support services to our schools.

In this next iteration of the HGfL the procurement of Internet services and connectivity for schools will be extended to provide an opportunity to include other Council sites with the aim of bringing the highest standards of service delivery to all whilst taking advantage of increases in scale and the latest technology to bring financial savings. The key features of our current requirement for schools are:

- minimum bandwidths of 16 Mbps for our smaller schools and 100 Mbps for our larger schools,

- web filtered access to the Internet to enable us to fulfil our eSafety obligations to our users yet with sufficient flexibility to allow schools to begin to take more responsibility for this web filtering where appropriate,
- an approach to security which protects the whole community of schools whilst proposing alternative approaches to particular school requirements and facilitating communications between the schools themselves and with the LA.

In order to achieve the required quality of service the Contractor will need to provide:

- very high service availability levels,
- detailed service documentation with online access to appropriate council staff,
- real-time on-line reporting of service delivery (such as bandwidth utilisation of individual circuits and aggregate demand for the Internet) with access to appropriate council staff.

Working with Hertfordshire schools

The Contractor must understand that Hertfordshire schools and other sites have a great variety of arrangements with regard to the provision of their on-site ICT support. The BSF schools and some of those managed by the Council's Schools IT Systems Support team (will) do receive a fully managed ICT support service. For other schools arrangements vary from relying entirely on their own technical staff to buying services from major educational suppliers through to local sole-traders. It's a mixed bag of support of variable quality which results in great variability across sites in the quality of the LAN infrastructure into which the Contractor will be supplying services. The Contractor must work within this complex environment to ensure that all schools and other sites obtain the best possible value from this contract. The "Trouble Shooter" service will be an important means by which the Contractor can achieve this through offering advice to schools where a poor user experience is due to inadequate local support and/or less than optimal local LAN infrastructure and end user devices.

BSF programme

Building Schools for the Future (BSF) represents a new approach to capital investment. It is bringing together significant investment (circa £45bn) in buildings and in ICT (Information and Communications Technology) over the coming years to support educational reform.

The contract for BSF in Hertfordshire will be allocated to a Local Education Partnership (LEP). In Hertfordshire there are 82 secondary and middle-deemed secondary schools and 25 secondary and all-age special schools that have been split into seven phases. The first phase of the investment will take place in Stevenage, which comprises seven secondary schools, three special schools and an Educational Support Centre (ESC).

The LEP will have responsibility for all ICT within the initial 11 sites comprising phase 1. This will gradually increase over a period of 12 years to include all those centres identified above.

In addition it is expected at this stage that the LEP will be responsible for the provision of an email service and Learning Platform (LP) to all Hertfordshire schools.

The Contractor will be required to work closely with the LEP and the Council to continue to provide network services to sites as they become incorporated into the BSF programme.

The Contractor will be required to agree and implement full inter-service incident management procedures with the BSF service desk.

From day one of the provisional BSF service ready date the Contractor must accept service desk calls from:

BSF ICT Managed Services provider
BSF Email provider (if sub-contracted)
BSF Learning Platform provider (if sub-contracted)

The Contractor will be required to agree and implement full inter-service incident management procedures with The Council's Managed Service provider and associated service desk(s) for corporate services delivered to the Schools in Hertfordshire.

Herts SITSS help desk

The Council's School IT Systems Support group (SITSS) will provide a Council "help" desk that all Hertfordshire schools, except those taking services from the BSF supplier, will use for first line support for all services delivered under this contract.

The Contractor's "service centre" desk will work closely with the Council "Help desk" to provide a seamless service to Hertfordshire schools.

2. NETWORK SERVICES

County wide resilient network

The Contractor will provide a fully managed wide area broadband network across the County to enable high speed communication to schools and other educational child/youth related sites.

In order to meet our overall business requirements the network will be based on an "LLU distributed network" approach with the design and implementation allowing the Council to securely operate a number of separate virtual network overlays over a single physical network infrastructure. The proposed solution will meet the following criteria:

- Value for money enabling high speed network delivery to small sites.
- Network nodes, used to terminate circuits to "end user" sites, will be located in secure, professionally managed and equipped network exchange sites or supplier hosting sites with resilient power supplies, environmental control and controlled 24 x 7 access. These sites will not be moved within the life of this contract.
- IP Ethernet technology (layer 3 switched)
- Resilient design
- High speed broadband circuits to all sites.
- Use copper, fibre optic (10, 100,1000 Mbps) and wireless technologies as appropriate
- ADSL and SDSL
- Any combination of services to be made available on any of the different virtual network overlays (see below for further information)

- Differentiated classes of service for different types of traffic.
- National or International high speed Ethernet presented IP based services available to connect to remote hosting or service delivery centres.

Resilient core distribution network

The requirement is for a single high speed secure resilient fibre core network linking "points of presence" and exchanges. The core network will have no single points of failure and be engineered to provide a minimum of 99.9% availability, calculated per calendar month, 365 days 24 x 7.

The schools core network should initially be capable of fully loading the two gigabit connections into the Internet. Core network bandwidth upgrades must be capable of being provisioned within 30 working days.

The Contractor will ensure the design of the core adheres to the Council's security policies, please refer to the attached appendices which detail the following documents

- The Council's security service definition
- The HGfL ICT security policy.
- The High level view of HCC security Policy

The Council will need to agree and sign off any design and reserve the right to carry out Penetration and Security tests on the network prior to final signoff.

Virtual network overlays

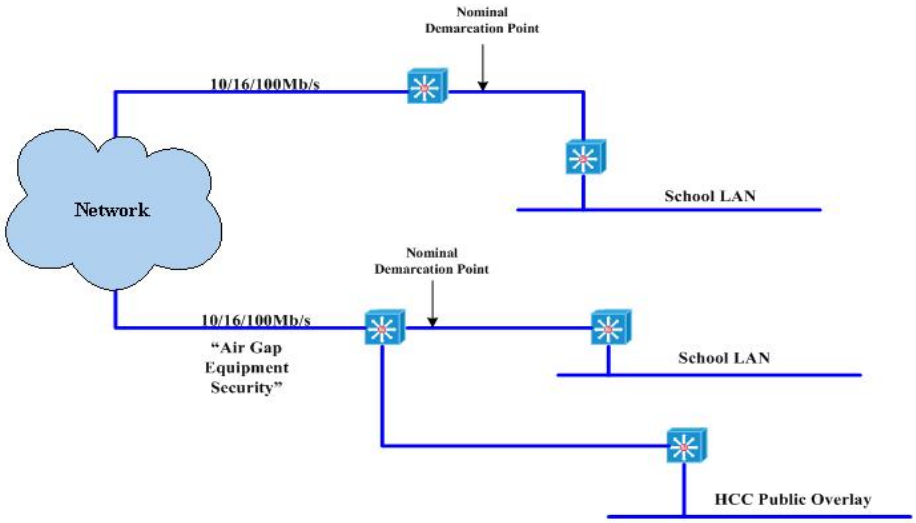
The physical core network will support multiple secure virtual networks that will enable the Council to maintain appropriate and separate networks for a range of different service environments.

Security level and techniques used to achieve this segregation across the new network must be equivalent to 'air gap' traditional physical security. It is anticipated that MPLS, Ethernet in Ethernet / Q-in-Q type MAN or other suitably accredited technology will be used to achieve this separation

The Contractor must be able to deliver the public, private, HGfL and other networks to the same site either by separate links or by local WAN switch on site.

Note: Standard 'LAN' based VLAN tagging as a way of achieving this segregation is not acceptable**.**

Site Level Services - Schools



EXAMPLES OF POTENTIAL SERVICES REQUIRED AND HOW IT IS ENVISAGED THESE SERVICES WOULD BE DELIVERED OVER COMMON SERVICES WHILST MAINTAINING SECURITY LEVELS

The network design will include the ability for additional virtual networks to be added or removed at any time during the life of the contract.

The proposed network design must allow provision for any overlays to be delivered to any site at any time to allow the council complete flexibility of use within its property portfolio.

Initially it is envisaged that the Council will require the following range of 'air gap ' equivalent securely presented virtual networks for the schools networking environment:

Schools network (Hertfordshire Grid for Learning)
A virtual IP based network overlay comprising 526 schools plus a variety of additional sites where the Council provides for the care and/or education of children that will allow all sites secure, appropriately web filtered access to education services and support located within the Council and on the Internet. Education facilities will include, but not limited to web filtered access to the Internet, email, web hosting, private learning material on the Internet, Learning Platform and MIS systems.

CCTV network overlay
This will provide a dedicated overlay for delivery of remote CCTV provider services to schools. Note: this will need to be deployed in conjunction with school level LAN changes (dedicated VLAN).

Public network
A virtual IP based network overlay, which will allow visitors to network attached sites to access the Internet via site based wireless networks and cable attached connections. This service will require a base level of web filtering.
This virtual IP based network will also be required to support The Councils public library sites to provide Internet services via an appropriately web

filtered service. This service will require a unique web filtering regime that adheres to the Councils Library Authorities standards.

BSF specific virtual overlay and dedicated services
A virtual IP based network overlay with ability to have additional point to point circuits/connections to enable local school consortia inter-working and to enable specific BSF services to be built. This overlay will also require web filtered access to the Internet for specific BSF related services. High capacity connections from the overlay or directly to a number of centralised hosting centres. Full interconnection with the HGfL overlay may also be required.

Network traffic prioritisation (Quality of Service)

The Contractor is required to implement Class of Service (CoS) to ensure prioritisation and bandwidth allocation guarantees supporting at least 5 CoS traffic types across the network. Prioritisation and class of service levels will need to be provided within the core network, for each virtual overlay and within each individual overlay.

The Contractor's network will use IP quality of service (QoS) to prioritise different types of traffic, ensuring that business-critical and real-time data does not suffer degradation regardless of the amount of other traffic on the network. Percentages of the total bandwidth will be reserved for each type of traffic, safeguarding the most important traffic streams.

The Contractor will undertake to define, monitor and modify as appropriate these percentages to ensure each network will deliver the best experience for the end users.
The Council wish to be able to prioritise data at network layers 2, 3 and 4.
Traffic shaping facilities may also be required to ensure specific protocols or activities either have sufficient bandwidth or have that bandwidth restricted to ensure these activities do not impinge on core services.

Note: Prioritisation and class of service levels will need to be provided within the core network and for each virtual overlay and within each individual overlay.

Access network to user sites - overview

Network attached sites will be linked to the core backbone network by circuits at a speed appropriate to their needs with a minimum of 16 Mbps using LLU copper, fibre and wireless as appropriate.

The requirement for links up to 30 Mbps is that they have an availability of 99.5**%**, 365 days 24 x 7. With latency measured to either core data centre that does not exceed a maximum of 40 ms RTD, with jitter no greater than a maximum 5 ms one way and a packet loss not in excess of 0.1%.

The requirement for links with speeds between 30 Mbps and 300 Mbps is that they have an availability of 99.5**%**, 365 days 24 x 7. With latency measured to either core data centre that does not exceed a maximum of 25 ms RTD, with jitter no greater than a maximum 5 ms one way and a packet loss not in excess of 0.1%.

The requirement for links between 300 Mbps and 1Gbps is that they have an availability of 99.5%, 365 days 24 x 7. With latency measured to either core data

centre that does not exceed a maximum of 10 ms RTD, with jitter no greater than a maximum 5 ms one way and a packet loss not in excess of 0.1%.

A lack of service fault will be raised if these quality targets, identified above, are not met for 50% of the core day.

Faults resulting in loss of service or significant degradation in the quality of the service to the site will be fixed within 4 hours.

The on-site CPE needs to be able to offer multiple separate connections to the WAN to enable those schools that operate a strict separation of curriculum and admin networks to continue to do so.

It is envisioned that this services will be offered in the form of a fixed price upgradeable package offering the following performance options-

Option 1a	Service to users located in domestic or very low speed environments (ADSL)
Option 1b	2 Mbps symmetrical service over traditional TDM technologies
Option 1c	10 Mbps symmetrical service over fibre
Option 2	16 Mbps LLU symmetric service
Option 3	20 Mbps LLU symmetric service
Option 4	30 Mbps LLU symmetric service over coax cable / fibre
Option 5	40 Mbps over fibre
Option 6	60 Mbps over fibre
Option 7	100 Mbps over fibre
Option 8	1000 Mbps over fibre
Option 9	10/100/1000 Mbps point to point circuit over fibre

Note: all services Ethernet presented.

The Council will provide the Contractor with at least 3 months notice of site closures and mergers. These will be handled through the service change process. Charges for circuits will cease on the day of disconnection and cancellations will not incur any penalty charges.

Schools and specified care sites

The Council's Children Schools and Family (CSF) department has 526 schools (nursery, primary, middle and secondary) plus a variety of additional sites including residential children's homes, and other sites where the Council provides for the care and/or education of children.

In addition the Council operates various initiatives that require them to provide secure access to web filtered Internet services from domestic properties and youth clubs. Currently this requirement is met using domestic broadband services and VPN access from locked down Council provided laptop PCs via a VPN into the Hertfordshire Grid for Learning (HGfL) network.

All secondary and middle schools **(see appendices for School site details)** will require 100 Mbps synchronous links into the core network giving access to the HGfL, corporate and public virtual network overlays.

All other schools and education sites with the exception of domestic premises and occasionally used sites will require as a minimum a 16 Mbps synchronous link **(see appendices for School site details)** providing secure overlay access into the HGfL, corporate and public virtual network overlays.

The Contractor will provide a low cost ADSL broadband service with a minimum speed of 2 Mbps to provide services to children in foster homes and youth centres. This service must terminate within the HGfL network overlay enabling secure web filtering access to the internet and other services available from schools networks.

Site analysis is as follows –

Site description	**numbers**	**Initial Circuit speed**
Primary, nursery and first schools	440	Min 16 Mbps
Secondary & middle schools	86	100 Mbps
Residential homes	11	Min 16 Mbps
Other centres (ESC) etc.	14	Min 16 Mbps
Domestic homes & youth centres	24 (to date)	ADSL broadband service minimum speed 2 Mbps

It is anticipated that the demand for network bandwidth to schools will significantly increase during the lifetime of this contract. Where the network service is provided over a technology that allows for an increase in speed by means of configuration changes then we expect these changes to be made without an upgrade charge. All upgrades of this nature must be remotely executable within three days of a request.

The Contractor is required to advise the Council of the maximum upgradeable capacity of each installed circuit at time of provision and to maintain online record of installed circuit base and upgrade capability.

Where the Contractor is unable to meet the basic service provision of 16 Mbps then they will –

- offer a similar service (speed and quality) using bonded, combination of or compressed technologies if possible
- make an initial proposal explaining the problems and offering the best connection possible for those sites concerned
- commit to producing a written review of these sites in the light of developing technology and services every 6 months

The Contractor will also be required to provide point to point circuits as and when required by schools to link disparate sites. BSF and partnership schools may require up to 1 gigabit dedicated links extending beyond Hertfordshire.

At the time this specification was compiled the following point to point network circuits, provided by NTL, were in place to facilitate split site operation. The Contractor will be required to replace /maintain these circuits.

A-end	B-end	speed
Barnwell School Barnwell, Stevenage SG2 9SW	Barnwell School Collinswood Road Stevenage SG2 9HQ	100 Mbps
St Michaels School St Albans (Top school) St Michael Street, AL3 4SJ	St Michaels School St. Albans (bottom school), St Michael Street, AL3 4SJ	100 Mbps
Sandringham School, The Ridgeway, St Albans, AL4 9NX	Beaumont School, Oakwood Drive, St Albans, AL4 0XB	1000 Mbps
Verulam School, Brampton Road, St Albans, AL1 4PR	Beaumont School, Oakwood Drive, St Albans, AL4 0XB	1000 Mbps
Sandringham School, The Ridgeway, St Albans, AL4 9NX	Verulam School, Brampton Road, St Albans, AL1 4PR	1000 Mbps

Resilience Requirement:

To improve network availability to schools the Council requires the following network resilience options to be made available:

- A low cost ADSL/SDSL backup that can be used in the event of the failure of the access network link to allow leadership and management staff at schools to access "key" business services like email, payroll, etc. This resilience option will come from the same exchange/node and offer full auto cut over and routing scheme integration.

- A bonded ADSL resilience option, that will come from the same exchange/node , with full auto cut over and routing scheme integration for all sites with SDSL and higher speeds. This offering must have the ability to bond services together to increase link speeds up to a minimum of 8 mbps.

- A full bandwidth triangulation option using backup links to other exchanges or via other technology and/or network infrastructure suppliers. This option must also have full auto cut over and routing scheme integration.

Schools will make their own decisions about whether to invest in this service therefore this provision could be requested at any time during the lifetime of the contract.

Customer Premises Equipment (CPE)

The Council expects that the Contractor would wish to provide onsite CPE equipment. If provided the Contractor will be responsible for the provision, installation, configuration and ongoing support of the Customer Premises Equipment and any additional equipment installed by the Contractor over the life of the contract that is on the Contractor's side of the demarcation line.

All CPE equipment must be capable of 19" rack mounting directly to racking frame. Also some sites will not have suitable racking and so the CPE must either be capable

of shelf or desk mounting or have a smaller footprint ‘small office’ friendly silent variant.
The CPE equipment should present a standard Ethernet RJ45 connection, assume 4 port/overlay capable at full bandwidth and be capable of 10/100/1000 Mbps operation dependent on scale / model.

The CPE should also be capable of L2 transmission and transmission of full L3 routing.
If the CPE itself can not act as a router the supplier will need to explain how the HGfL Layer 3 network interconnectivity and routing plans will be maintained across the new NW. Where local routing will take place and how sites with multiple resilient connections will achieve automatic routing and auto failover.

All Customer Premises Equipment must support SNMP standard traffic and error statistics.

All CPE equipment running at 10 mbps and above must support the more detailed traffic monitoring and analysis capabilities of “Sflow” or superior open/multi-vendor standards.

The Contractor will remotely manage all of the school CPE equipment. This will include configuration (changes will be handled through the engineering change control process), software upgrades, security, performance & error/fault management.

The Contractor will ensure that CPE equipment software versions are upgraded so that they will support the functionality required to meet school’s service requirements and always be within two fully supported ‘bug free’ releases of the manufacturer’s most up to date release. All service issue related upgrades for CPE firmware, software or hardware will be included in the contract and carried out at no additional charge to the Council. .

Some schools operate separate Admin and Curriculum LANs. This situation may well continue. These are both networks on the School / HGfL overlay but they may have different security approaches.

Routing restrictions, ACLs or other embedded or NW associated controls will be required to enable the sensible control of security issues such as virus outbreaks as well as a general restriction on inter school access. Individual schools or groups of schools may wish to relax the restrictions in place for business reasons and the service request change process will need to be followed to ensure authorisation is provided for any reduction in base line security.

At this stage the Contractor should assume the following guidelines:

- no access is allowed from any Curriculum LAN to any Admin LAN where present
- no access is allowed from any Admin LAN to any other schools Admin LAN
- no access is allowed from any Curriculum LAN to any other schools Curriculum LANs

- where access is allowed from any Admin LAN to any Curriculum LAN connections are not allowed to be originated in the reverse direction

- access is only allowed from “external” address ranges to curriculum LAN but only after a security risk assessment and design agreement meeting. These changes must be signed of by the Council network design authority

- access is allowed from “external” managed VPN connections. These changes must be signed of by the Council network design authority
- no access from “external” address ranges to Admin LAN

- the ability to rate limit and if necessary prevent ICMP traffic from schools on to the network core is required (applied on site access switches)

There are some exceptions to these basic rules. For instance, where schools have a video conferencing solution, the access list has been modified to allow curriculum to curriculum access. At time of service rollout these controls will be agreed by the customer up on a school by school basis.

Current IP addressing schema (internal)

The Contractor will support the existing IP addressing structure used by the Council’s schools and other sites and work with the Council to implement changes as required over the lifetime of this contract.

All Council schools currently operate on a single “172.” TCP/IP address structure with a range starting at 172.16.20.0 and ending at 172.27.3.255. (See TCP/IP address table in the appendices for details of school allocations). Due to school equipment restrictions and to reduce effort for schools during the migration the authority wishes for the current IP allocations to be carried forward where needed into the new service.

Note:
This will have implications for interschool routing and in turn require specific groups of sites to migrate at same time as these IP ranges will also be present on the existing Contractor’s network.

To simplify administration on the firewall and routing devices it is currently recommended that schools use common addresses for network devices that are accessible from outside of the schools network. The current proposals are as follows:

Last IP Octet	**Use**
.254	CPE Switch
.253	Circuit proxy/Firewall
.252	Spare
.251	Server1
.250	Server2
.249	Server3
.248	Server4
.247	Server5
.246	Spare
.245	Proxy
.244	Email server (SMTP)

Last IP Octet	Use
.243	Web Server
.242	Video Conferencing 1
.241	Video Conferencing 2
.240	Video streaming
.239	Easy Trace Polling PC
.238	Easy Trace Server
.223 to .237	Reserved

The Council will review these recommendations with the Contractor before implementation to maintain a standards based reserved range allocation. The council is also developing a common LAN and local web filtering design standard that will be adopted and supported by all parties providing services to schools. The IP scheme and local services will be extended to incorporate: site switch CPE, site web filtering equipment, site firewall equipment, site LAN (multiple L3 subnets) and site WIFI (secured to multiple VLANs) and other equipment as required.

The Contractor must provide a mechanism for the upgrade of sites total IP subnet allocation. Extending ranges for Layer 2 LANs and adding additional subnets and restructuring subnets to allow for Layer 3 site LAN configurations. There are currently some address ranges that are duplicated within both the schools and corporate networks and these are reserved in one or other environments. In order to simplify this situation the Council wishes to introduce additional addresses in ranges outside those currently in place.

The Contractor will administer, enhance, manage and maintain records of the schools TCP/IP addressing schema.

Service demarcation points

For those secondary school sites that will be supported by the BSF supplier the network demarcation point for the Contractor will be the LAN port on the customer premises switch equipment supplied under this contract. The cable plugged into the port on the CPE will be supplied and supported by the BSF managed service supplier.

For non BSF schools the network demarcation point for the Contractor will be the LAN port on the customer premises equipment supplied under this contract. The cable plugged into the port on the CPE will be supplied and supported by the school/IT support arrangement. Schools manage their own ICT support arrangements and the range of provision is diverse and includes school's own staff, small single trader support, small and large support companies or the Council's own traded support organisation (SITSS).

This demarcation point will move in line with additional optional services supplied by the Contractor on a site by site basis.

If an on site web filter service is provided by the Contractor then the demarcation point becomes the port the school LAN/firewall will plug into on the Contractor supplied equipment.

If an on site firewall service is provided by the Contractor the demarcation point becomes the port the school LAN plugs into on the Contractor supplied equipment.

High speed links into existing corporate core network

The Contractor will provide two high-speed (gigabit circuits/connections) to the Council interconnect points located at Farnham House, Stevenage and County Hall, Hertford presenting the following (virtual) networks Public, Schools (HGfL) and BSF overlays.

High speed links into remote hosting or service delivery sites.

The Contractor will be required to provide National or International high speed Ethernet presented IP based services to connect to remote hosting or service delivery centres as required throughout the lifetime of the contract. The required services will be defined after the contract has started.

Network connections to other Networks

The Contractor will be required to provide network links to other networks whilst ensuring that their solution provides protection against interconnection. These networks will change over time but initially it should be assumed that the only connection will between the Council's corporate and Schools HGfL networks. The demarcation point will be as specified in the corporate part of this tender. If however the Council does not wish to take corporate services as part of the contract this interconnect will still be required.

JA.Net (NEN)

The Contractor will provide a flexible solution that will allow Hertfordshire schools to access the National Education Network and its services.

The Council has a 100Mbps circuit to JA.NET terminated at Farnham House, Stevenage. Provision of a JA.NET interconnect will be required, either via the Contractors core network or via the council's connection at Stevenage. The Contractor will provide routing and firewall equipment to allow interworking to a range of services including video conferencing (E164, H323 and SIP) over JA.NET. The Contractor must carry out IP network address translation and conform to JA.NET guidelines when providing interconnect to JA.NET

Financial services

The Contractor must provide connectivity to The Councils financial services provider, currently this is LOGICA CMG based in Bridge End, Wales.

Access to this service is currently over the Internet however as this is a critical business service, the Contractor will be required monitor this service for availability and responsiveness with the data being available on-line in near real time to the Council via a web browser.

3. CENTRAL INTERNET SERVICES

The Contractor will provide a resilient Internet service, DNS, web filtering and security (firewall, intrusion/denial of service protection etc.) for all users of this network who are allowed access to this service. These services will be fully resilient with no single point of failure, providing a minimum uptime of 99.99%.

The services will be provided on dedicated appliances which will have a hardened OS and will be running on high quality purpose built hardware. The services will all be scalable to N+1.

This service will be split across two physical locations; both with commercial hosting type faculties i.e. UPS, standby generators, cooling, access control etc with no single point of failure. The split across the two sites must ensure that all services will continue, even in the event of a disaster, whereby one of the sites could be unavailable for a long period of time e.g. a fire.
The core distribution network will have resilient links into the two separate physical locations The underlying infrastructure including Internet links must be able to extend to meet future growth in demand.

For service resilience those additional services (VPN, video conferencing ….etc.) identified in this requirements specification will also be located in both physical locations and will operate in such a way that a failure in one location will not cause a loss of service.

Internet connectivity

The Contractor will provide a fully resilient, load balanced, Internet service with services from two separate ISP networks, one located in each core site. The service will be designed and implemented to provide 99.99% availability 24 hours 7 days a week. The design will incorporate mechanisms to ensure that the service and all resiliency features are continuously monitored for availability and capacity. Availability, capacity and response monitoring will be made available to the Council in "near-real time" via a browser from the Council network and the Internet via a secure login.

The Councils initial requirement is no worse than current provision. This is delivered on 2 x 1Gigabit uncapped bearers. During the school day Internet traffic is peaking at 400 Mbps measured as a 5 minute average. It is expected that this traffic level and user profile will change over the length of the contract.

The Internet service must be designed to support future growth in demand without incurring the Council in any significant set-up or upgrade costs.

The Contractor will provide details of overall capacity available, ISP peering point information and class / tier of bandwidth provider used to deliver the HGfL/Schools service.

Firewall service

The Contractor will supply, maintain, update and configure an appropriately sized resilient "Firewall Service" located at appropriate points within the network to protect the network, services and users against "abuses" from the Internet and to protect and maintain internal/external network and service boundaries. The firewall service must be constructed in such a way as to offer a "per service" firewall. This means that any dedicated or detailed service such as video conferencing access should have its own firewall arrangement and this firewalls performance or configuration must not impact on or restrict the other services requiring firewall protection.

The Contractor will make changes to the configuration of the "Firewall Service" to support the delivery of network services to and from the Internet and to and from any other attached networks such as the National Education Network.

The Contractor will undertake to provide external IP address translation for those services that Hertfordshire schools require to be available from the Internet.

The “Firewall Service” must be capable of supporting additional DMZ’s and potentially links to content and/or other service/school suppliers.

The Contractor will be required to undertake IP address translation as required to other external networks.
The “Firewall Service” will be maintained so as not to be a limitation on the demand for Internet and other services passing through it.

Optional requirement - School level firewall -

The Contractor must offer a service to provide a fully managed local on-site firewall. This will be a single site level device. It must also provide NAT services and offer protocol level web filtering. It must also support a minimum of 5 separate interfaces with at least 2 of these being able to offer ‘dirty’ side services.

The Council cannot at this stage identify which, if any, schools will take advantage of this offering.

Anti-virus protection

The Contractor will provide, maintain and support a network anti-virus solution on a 24 x 7 x 365 day a year basis that will operate within key network areas to manage and restrain any virus outbreak.

Ongoing proxy service

All schools in Hertfordshire along with many other sites and partners rely on a “proxy service”. The new service must allow this to continue. The Contractor will provide and maintain a number of pre-determined proxy points as well as providing the ability to deploy “. PAC” files for traffic management and routing. Both the maintenance of the “.PAC” file and delivery mechanisms must be provided as a managed service.

Reverse proxy service

A reverse proxy service must be provided at both core 'Head End' nodal Internet entry points to allow both HTTP and HTTPS internal services to be made accessible from the Internet in a more secure fashion. Incoming website traffic and other school level system access will need to be made available through this mechanism.

The proxy server must be capable of passing HTTP traffic, terminating and rewriting URLs and forwarding traffic to both internal and external locations.
The proxy server must be capable of passing HTTPs traffic , terminating and rewriting URLs and forwarding traffic to both internal and external locations.
The proxy server must be capable of terminating HTTPS connections at the proxy with the ongoing connection being HTTP.

It is envisaged that the initial service will need to provide 1x HTTP incoming URL mapping per school (600) and 1 x HTTPS incoming URL mapping per
school (600) with a likely concurrency rate of 40 services mapped each with 12 active connections across all the schools.

Within the first year it is expected that this would rise to 100 concurrent services mapped each with 22 active connections across all the schools.

Please provide a design to accommodate this requirement, clearly explaining how the service could scale over the life of the project. Include options for future HTTPs acceleration
and any impact on design for other services included else where within the Tender.

Include details on Certificate supply and management and processes for adding , delegating or adjusting configured services.

Internet access – web filtering service

The Contractor will provide secure web filtered access into the Internet offering a range of environments appropriate to support: -

Learning in schools: The web filtering must offer an environment that needs to be safe and appropriate for children of different ages to use. The national standard for this is set by Becta. The Contractor must be capable of achieving the Becta standard if required although it is likely that the Council will choose to vary that standard for implementation.

Out of core hour school use: Use of schools in evenings and weekend by a range of age related users.

Home access use by staff: Application of similar school level based service to enable staff to produce learning materials at home confident that they will work once deployed in the school.

Home access use by children: Appropriately age restricted access.

Foster child use: Appropriately age restricted access.

Youth centre use: Appropriately age restricted access.

Public Library use: separately defined Web Filtering policy for use within The Councils Library establishments or via The Councils Public WIFI network. Age based restrictions with an option for a Microsoft Active Directory linked policy application linked to The Councils Library PC control system.

General service requirements –

The Council will determine the policy on web filtering and the Contractor will be responsible for its implementation.

The Contractor must provide a resilient web filtering service which will supply, as a minimum, the following for all schools:

- web filtered access with a choice of Web Filters based on proxy settings in the browser
- one of these policies will be the "baseline" policy which will form the least restrictive policy available at any school or Council site .
- all accesses made to services on the Internet must be logged by source IP address

Some schools may wish to add local solutions with the ability to set their own web filter options above the “baseline” web filtering.

In failure situations the Internet web filtering solution will either default to the “baseline policy” as determined by the Council or will completely block all access to the Internet.

The solution will provide the Council with detailed reporting on usage and traffic patterns logged by source IP address. The detail of the reporting will allow the Council to identify malicious users on the network and respond promptly. The statistics and reporting will furthermore give the Council the capability to monitor user behaviour and general trends and enable them to plan accurately for the future.

Categorisation of web sites

The solution will index the entire World Wide Web so that all sites are categorised.

When uncategorised sites are first requested by a user on the Council network this must trigger a mechanism whereby the site will be categorised within two (2) days.

The solution must support the ability to ban or accept uncategorised sites on a global or individual basis.

The ability to deal effectively and rapidly with new "anonymising proxy" sites will be a critical factor. The solution deployed must demonstrate its use of forensic style techniques to ban access to both client and clientless proxy avoidance sites

The Contractor will provide a service that, when requested by school representatives, will ascribe local categories to sites that over-ride the categorisation used elsewhere by the web filtering solution. The Contractor will agree the operational process required to deliver this service in a safe manner with the Council.

Changes to central web filtering policies and local changes to website categorisation will be completed within 1 hour of the request being made by Council representatives.

Web filtering policies

The Contractor will provide a central system that offers schools a choice of web filtering policies accessible by browser proxy settings.

Web filtering policies must be possible through allowing and denying the different categories as well as allowing and denying individual sites. all web filtering policies must be capable of choosing a default position with regard to uncategorised sites by either allowing or denying them.

One of these policies will be the "baseline" policy which will form the least restrictive policy available at any school or Council site. This “baseline” policy will be determined by the Council and implemented by the Contractor.

There must be a mechanism for the Contractor to over-ride any decision on categorisation of a particular site made by the web filtering supplier. The solution must be able to provide up to ten (10) of central policies which will be set by the Council, which schools or other users can use by a simple configuration change such as browser proxy settings.

Web Filtering policies and user differentiation must be possible by source IP address or subnet.

Image searching and safe mode

The web filtering solution must be capable of determining the source of each image produced by an image search (provided of course the source is advertised by the search engine) and then applying the relevant active web filtering policy to determine whether or not each thumbnail produced by the search should be displayed i.e. thumbnails of source images which would be denied under the active policy must be blanked out leaving allowed thumbnails to be displayed.

Where a search engine does not advertise the source of its images in an image search there must be the capability to deny that search engine's image search facility entirely within any web filtering policy.

Where a search engine offers its own "safe mode" or "family friendly" mode the Contractor must be able to force that mode into the "on" position within any web filtering policy. In this context "force" means "over-rides whatever mode was chosen by the user". (In general the ability to re-write URLs as they pass through the Web Filtering and/or proxy solution will be an advantage.)

Video content Filtering Portal

The Contractor must be able to Filter access to on-line video sites such as “You Tube” and provide the Council with the ability to publish on a portal and/or allow access to specific video clips that contain Educational content.

A management classification and publishing service must be provided within the contract.

HTTPS (man in the middle) filtering

The Contractor must be able to allow for blocking/Filtering, interception and decryption /interrogation of all HTTPS traffic with full activity reporting as per HTTP services.

FTP filtering

The Contractor will provide a resilient FTP proxy service to all schools.
As a default all FTP Internet traffic will be blocked except for those sites held on an FTP allow list.

The Contractor will maintain the allow list but requests from schools will initially be referred to the Council for approval.

Browser based FTP services must be Filtered with the ability to restrict destination by URL or IP address.

In addition the ability to packet shape or restrict bandwidth available to proxy based or browser based FTP services is required.

Protocol filtering and packet shaping

The internet service traffic profile may require the Council to restrict the use of certain protocols or activities, such as Internet Radio, at peak times or in line with the working day or extended schools agenda.

The Contractor will offer an option for the filtering of Internet services by protocol, IP port number and throughput. Shaping traffic will restrict throughput by time of day, port used, protocol used or combination of the above to create a recognised service such as peer to peer sharing. The solution must be granular and allow for throughput restrictions up to complete restriction, in effect making the service unusable.

Web filtering - Monitoring and recording

The Contractor is required to provide the ability for designated Council staff to monitor Internet access in real-time with the ability to select particular schools, particular categories of website and/or particular infringements of web filtering policy.

Logs of all web access must be kept in easily accessible format for thirteen months with instant availability. It must be possible for designated Council staff to interrogate these logs with access to information about client IP address, URLs accessed, time and user input. Where Active Directory integration exists we will also require user login credentials to be held within the logs.

After thirteen months logs will be archived and retained, in secure off-line storage, for a further seven years in such a way that they can be retrieved for review if required. Archived data will be made available for analysis and reporting within 5 workings days of a request.

The Contractor should provide information from the logs only to designated Council staff and/or the police when authorised by the Council or court order.

Option to make use of existing HGfL web filtering solution currently deployed by NTL

The Contractor should indicate whether they would be willing to deploy the existing Fortigate solution to provide resiliency for the solution offered or as part of the proposed service.

The existing central Web Filtering service, implemented in 2008, is based on Fortigate solution (2 x FortiManager 3000 management systems, 1 x FortiAnalyzer 4000 system (4.8 Terabit Storage System) event logging and reporting platform, 1 x FortiGate 5140 14 slot chassis,4 x 5001 application blades, 2 x switch blades, 2 x power supplies). This service supports 5 different Web Filtering policies which allow the user to access certain categories of website and deny access to others. For further details of the solution and Web Filtering categories see additional information -HGfL Service Catalogue contained in the appendices.

Optional requirement - School level web filtering -

The Contractor must offer a school level web filtering solution. The Council cannot at this stage identify which, if any, schools will take advantage of this offering.

The solution must be capable of being applied as a local service in an individual school or site should they want to manage their own web filtering policies. These schools will use the baseline (minimum web filtering level) feed into the school on which they will apply their own local Web Filtering.

Schools then define all their own web filtering policies for individual users and groups of users, individual machines and groups of machines and particular times of day developing reports and statistics as required. These will be offered as a fully supported local solution with full management capabilities.

The local solution should be capable of integrating into the schools Windows server active directory services or other open standard directory services for further user differentiation.

The service must offer web filtering by Active Directory group and scheduled time of the day for groups and individuals as the minimum requirement.

Option to support school based FortiGate web filtering solutions

A small number of schools also use a local FortiGate 200A (10 schools) and 300A (30 schools) working in conjunction with the central solution.

The Contractor should indicate whether they would be willing to provide hardware and software support, repair and maintenance only, for these devices located in Hertfordshire schools.

The service offered should cover the ability to:

- take a nightly equipment backup for a rolling 5 days period
- roll back the configuration in 24hr steps up to the full 5 day period
- return the service to its installed base configuration

Note: Schools will be expected to control the policy locally and make use of the roll back options if they get into trouble and can not resolve any issues caused due to changes in their local policy / configuration.
Although the Council would expect some basic advice and guidance to site managed filtering installations the expectation is that the Contractor can simply ‘roll back ‘after a local configuration has become corrupt or unsuitable/stable.

For further details see the “HGfL Service Catalogue” contained in the appendices.

Content cache service

The Contractor will provide a fault-tolerant and fast caching proxy solution in order to speed up delivery of content to users, reduce the amount of Internet capacity required and reduce network load.

The solution should support HTTP, SSL (Including SSL Intercept and Inspection), Streaming Protocols Real Media (RTSP), Windows Media (MMS), and QuickTime over HTTP, FTP, SOCKS, AOL, MSN, Yahoo Instant Messaging Clients, TCP Tunnelling (SSH, Telnet, TFTP) and be capable of caching HTTP, HTTP Streaming - Unicast and Multicast, HTTPS, FTP, MMS - Unicast and Multicast, RTSP - Unicast and Multicast, and QuickTime over HTTP.

The solution must be based on a platform that will be continually enhanced to reflect protocol developments on the Internet and not be a limitation to the schools access to Internet services.

The Contractor will ensure that the web filtering and caching service linking the schools network to the Internet is maintained and enhanced in line with Internet access capacity so as not to restrict throughput.

Note: The Council's current HGfL service operates a cache solution and achieves a reduction in Internet bandwidth of between 30% and 40%. Cache provision is at the discretion of the Contractor. However if a non cache solution is proposed the council will require a 40% reduction in Internet bandwidth charges.

Reporting

Each month the Contractor will report on the effectiveness of the caching service: Providing weekly and four weekly summary details of-

- the amount of network traffic that was cached in total and by protocol
- the amount of network traffic that was not capable of being cached in total and by protocol
- the actual amount of content retrieved from cache in total and by protocol
- provide details of the time taken to retrieve content from the cache
- provide details that show the loading of the cache service in terms of the overall capacity
- in summary the reports should be able to demonstrate what bandwidth saving the cache service provides and what impact it has (positive or negative) on performance

Trend analysis reports covering a thirteen month period will be required for all of the reports listed above.

Option for the Contractor to make use of the existing HGfL caching solution

The Contractor should indicate whether they would be willing to deploy the existing caching solution to provide resiliency for the solution offered or as part of the proposed service.

The existing cache solution is base on 2 Zeus ZXTM-LB load balancers and four Blue Coat ProxySG 810-20 appliances.

For further details see the "HGfL Service Catalogue" contained in the appendices.

Network and Internet security

The Contractor and the Council will agree the web filtering and security policies, adhering to the Council's security principles, governing the delivery of network and core services to Hertfordshire schools and other sites.

The firewall security policy will be agreed with the Council and no changes will be made to the policy without prior written consent from the Council's Designated Technical Authority.

Firewall services must be provided on a service by service basis so that technical restrictions and resulting firewall configurations do not impinge on each other. Restrictions to one service (e.g. video conferencing) must not place technical or operational restrictions on another.

The policy controlling content web filtering will be determined by the Council and implemented by the Contractor. No changes will be made without prior consent from the Council's Designated ESafety Authority

The Contractor will maintain/enhance the security on their network to counter new threats from the Internet community and will exercise due diligence in identification and the taking of remedial action against all such threats.

The Contractor will have contracts with the suppliers of relevant hardware and software used to deliver the Service for the provision of security updates and patch information. Important security patches will be implemented within 24 hours of notification. Where such patches require a maintenance interval to complete, these shall be scheduled to provide minimum interruption of service during core times, whilst remaining within the required response parameter.

The Contractor will ensure that equipment software versions are upgraded so that they will support the functionality required to meet schools service requirements and always be within two fully supported 'bug free' releases of the manufacturer's most up to date release. All service issue related upgrades for firmware, software or Hardware will be included in the contract and carried out at no additional charge to The Council.

The Contractor will provide the necessary technical resources to periodically review (at a minimum quarterly) network security with the Council, document and implement any agreed changes. Changes will be managed through the change control process.

The Contractor will hold quarterly meetings with the Council's school and corporate security staff to review developments, progress and new threats.

The Contractor must work with the Council to enable the Council to undertake full auditing of the service. Also the Contractor will allow the Council or it's agents to carry out both external and internal penetration testing. Providing full access to the data centre/s and or POP/exchange sites as required.

The Contractor will notify the Council (names and contact procedure to be agreed with the successful Contractor) within 1 working hour of a security violation being detected with recommended remedial actions. A written explanation of each violation explaining what happened what subsequent action was taken must be made available for review at the next account meeting.

Access control lists and IP routing restrictions

The various IP overlays will be separate from each other and any inter-working will only be allowed via central Council controlled firewalls. However within an overlay the council will require site to site and site to service IP restrictions to be provided by agreement. Traffic flow will need to be controlled/restricted by the use of ACLs, IP Filters and/or routing restrictions. Control should be per subnet, by range of subnets by address port and protocol.

DNS service

The Contractor will provide and maintain a resilient DNS service (internal and external) on a dedicated DNS platform based on the latest industry standard platform. The platform will provide centralized DNS records and distributed resolvers for optimized performance and resilience. The DNS configuration will provide full resilience with automatic switch over in the event of service failure.

The Contractor will need to both integrate and filter out local Microsoft DNS registrations. The Contractor will produce an agreed standard with the council and offer advice and guidance to schools on the set-up and configuration of local network DNS systems/servers.

The Contractor will provide an internal DNS resolution. This will include internal re-directed services into the Council's corporate network for both the council corporate internal and external addresses as needed.

Internet domain management

The Contractor will provide the Council with a domain registration service for "org" and "org.uk domains and offer a "help desk" and a registration service for ".herts.sch.uk" domains if required by the Council's schools.

The Contractor will be responsible for the provision of authoratitive DNS for those Hertfordshire's ".herts.sch.uk" domains covered by this contract and any other domain that may be required by the Council.

Note: Not all "herts.sch.uk" domains are owned by Hertfordshire Council schools. Some belong to Independent schools located in Hertfordshire

Internet addressing

The Contractor will supply and maintain sufficient "real" Internet TCP/IP addresses to enable Hertfordshire schools to provide, participate in and make use of services offered over the Internet.

At present the Council's schools network has approx. 285 public IP external addresses used by Hertfordshire schools for a variety of purposes – see the appendices for the list of "Schools Public IP Addresses supported by NTL"

The Contractor will undertake to provide external IP address translation for those services that Hertfordshire schools require to be available from the Internet and provide as many additional public TCP/IP addresses as required to implement new services throughout the life of this contract.

It is anticipated that the address range will need to increase by 200 over the next two years.

Changes will be authorised and requested using the “change management” service provided to Hertfordshire schools by the Contractor.

Service Performance and availability reporting Service for the Council

The Contractor will establish and maintain an online IP network performance reporting service to provide the Council with real-time information on the current and historical performance of their networks ideally accessed via a browser.

The IP reporting service will provide on-line “near” real time, evidence of ongoing performance showing internet and individual line usage showing traffic flows in both directions presented in 5 minute intervals across all technological platforms deployed to deliver the service. This should be in the form of statistics derived from network equipment and or external probes.

The IP reporting service will provide a wide variety of pre-defined reports in easy-to-read tabular and graphical format, with information at both network and site level. Both summary and detail reports, and tools to help focus on the time periods and groups of devices or sites that are of particular interest.

The IP reporting service will hold 13 months of historical data for sites including figures on latency between elements of the core network, percentage utilisation and round trip delay between core and all network components. This information is to be available in both graphical and tabular form. The service will support five years history and trends for main items.

The Contractor will provide details of the interface and any web components required by the client software. If the “tool” uses a thick client then the Contractor must provide full details of the software, licensing, operating system and hardware platform needed to support the client software.

The Contractor must provide monthly test results showing:

- performance testing results against agreed targets that demonstrate that there are no bottlenecks within the core network
- that full bandwidth is available from all outlying sites to the local connection point or node. (i.e. each remote site can simultaneously load their links to capacity)
- that the core network can be loaded to its design capacity.

Provide an online “traffic light” graphical /tabular presentation showing the service status of all sites and key network components. Schools and the Council should be able to view the status in real time. The online status must have a clear demarcation between the school first contact point and onsite supplier equipment.

The on-line reporting tool will be made available both within the network and from the Internet using a web browser and username, password and PIN number.

Online historic up/down and quality status reports must be made available to the client function within the council.

The Contractor will provide an on-net self diagnostic and performance testing facility for schools that will:-

- allow schools to perform bandwidth tests between their CPE and the Internet and “key” core interconnection point

- allow school IT staff to run real time upload and download bandwidth tests and present these results through a browser interface as part of the testing process

- provide online user perception / user journey taken reporting. This will consist of a centrally located monitoring point that will provide details of the path travelled/ internet journey measurement to a basket of agreed web hosts. The network will deliver 95% of all user path travelled journeys within 1 second. It will monitor a basket of web sites. The basket will consist of 10 Cached and 10 non cached sites. A thirteen month tabular record of this performance will be provided by the Contractor.

- allow schools to view the “quality” of their network link to include latency, jitter and packet .

- an optional school located user perception and performance monitoring point is also required. This will consist of a school level device located within the school that will provide a user, located within that School site, with details of the path travelled/ internet journey measurement to a basket of agreed web hosts. The network will deliver 95% of all user path travelled journeys within 1 second. It will monitor the same cached and non cashed sites as the central service.

The Contractor will provide a baseline web restriction checking service. This will consist of a centrally located monitoring point that will measure to a basket of agreed web hosts. The basket will consist of 10 Cached and 10 non cached restricted sites as defined in our Web Filtering base line configuration. The service will generate an ALARM should any banned sites be accessible.

The Council will be notified and a fault will be raised by the Contractor within 30 minutes of the alarm being set off.

(Note: The Contractor and the Council will agree an action plan depending on the nature and severity of the failure.) A thirteen month tabular record of this performance will be provided by the Contractor.

The Contractor will agree and as appropriate review and revise “benchmark” figures with the Council that can be used by staff at sites to evaluate any test results provided by any elements of these services.

.

The service Performance and Availability Reporting services as defined within this section of the specification should be made available to all other corporate network overlays in a way that does not compromise security and is in line with the Council’s security policy.

4. ADDITIONAL SERVICES

The Contractor will supply the following additional services.

VPN Service

The Contractor will provide a fully managed SSL and IPSEC client and clientless VPN service that will:

- Allow users to access network services from outside the network using an Internet connection.
- Allow for secure school to school access.

The VPN solution will need to include an optional email and text based two factor access security service. Users will need to have a username, valid complex password and monthly text or email access code to gain access to the network. This service will meet a range of different needs including, but not restricted to:

- school administrators requiring access to manage school systems
- technical support staff requiring access to manage networked systems with outgoing internet services.
- allow teachers to update MIS from home outside school hours.
- allow staff (CSF, Corporate and partners) to work from home
- allow school staff, located outside the school, to access the Internet through the schools web filtering service in order to check accessibility in schools.
- provide access to an Internet "walled garden" for foster children and youth clubs.
- third party support for services located on school networks.

The service must deliver DNS and DHCP full scope and extension variables (including all standard Microsoft and VOIP related). The service must provide access to the full range of HGfL services.

The service must be resilient with a suitable fail over mechanism to ensure service availability.

The service must carry out inline antivirus checking for all incoming access once connection is established and traffic is in an unencrypted format. Full AV and endpoint security checking is also required for machines using SSL clientless access.

The Contractor will manage the registration and maintenance (changes and removal) of user accounts and associated security services working to a process agreed between the Contractor and the Council. A user "self service" facility will be provided to enable those authorised staff in schools and other establishments to "auto" register and change their contact details (telephone, mobile, email etc.) as a way to streamline the process of managing large numbers of user accounts required for services like VPN.

The Contractor will be required to make available on-line up to date clients and appropriate documentation for school users of Microsoft, Apple and Linux operating systems.

The Contractor will support full account management and provide restricted level user support to school staff.

Support will consist of advice and guidance and 'hand holding' for staff access issues during the hours of 8am to 8pm Monday to Friday. The support will be brokered via the HCC SITSS 1st level help desk and will typically be agreed by appointment in advance. It will consist of support and assistance by telephone and email to users experiencing connectivity and remote client installation, configuration and commissioning issues.

Also the Contractor will be required to provide and support a test facility to enable the Councils (SITSS) service desk to test that the service is working at any time. This facility will also be used to perform daily testing of the service as part of the service desks regular maintenance routines.

The solution should initially be sized to support up to 6,000 user accounts and up to 600 concurrent sessions with the capacity to be upgraded, if required, within three months of the need being identified.

For added security any SSL and web based VPN services must operate through a reverse proxy or security gateway with inline antivirus and intrusion detection protection deployed.

The Contractor will provide the Council with secure on-line access to reports showing the registered users (name, groups and totals etc) and daily usage details to include who was signed on and duration of session and IP addresses accessed.

This service will be setup in such a way that "split window" operation will not be possible for staff, supplier and "walled garden" access.

Staff will be able to access school systems and the Internet via this service. IP Filtering or ACL policy control must be available for deployment on the VPN equipment

It is envisaged that the Head Teacher or Site Manager of each school and an appropriately authenticated person from approved organisation will nominate a person to manage their VPN user accounts. This person will make a formal request for their school or organisation to be set-up on this service by completing the appropriate service request form.

Once approved, users from the school or authority will be able to register their own details on-line. This information will be confirmed on-line by the authorised representative for that school or organisation prior to being accepted.

The system will operate using passwords adhering to Council security standards and the aging out of passwords and unused accounts. It will also allow the person responsible for managing the system to review, on-line, the details of users registered to their school or organisation and remove as appropriate.

VPN Training

The Contractor will also be required to produce an on-line training module for all VPN facilities. This must also be in a form suitable for deployment on the Council intranet Technical Wiki.

Video Conferencing Service.

The proposed solution must support H323 and SIP based services as well as offering an MSN and Skype gateway. It should also address other emerging technologies for video conferencing such as those offered by Google.

The Contractor will provide a resilient and robust IP video conferencing solution that will allow schools to engage in point-to-point and point-to-multipoint video conferencing sessions with:

- Schools and sites located on the Hertfordshire schools network
    - Via the Council's MCU
    - Using H323 and SIP Point to Point (Initiated on an outgoing basis and received as an incoming on Net connection).

- Schools and sites on the Regional Broadband Consortium networks and NEN
    - Via the Council's MCU
    - Using H323 and SIP Point to Point (Initiated on an outgoing basis and received as an incoming on Net connection).

- Schools abroad over the Internet
    - Via the Council's MCU
    - Using H323 and SIP outgoing and incoming

- Skype, Google and MSN public video conferencing inter-working.

  Notes:

  It is anticipated that specialist session controllers, Voice firewalls and gateways will be used to deliver this service so as not to damage Network Security.

  Skype inter-working must be carried out in such a way as to restrict bandwidth "grabbing" by Skype to 512 kbps per live user including the live connection/conference.

- Video conference end points located on the Internet (H323 and SIP outgoing and incoming)

- ISDN connected video conferencing end points.

All video calls must have the ability to use E164 addressing to communicate on net and with the national and international E164 based infrastructure available over the Internet and JA.NET.

The proposed solution must operate using the H460 standard for firewall traversal/split gateway technology to ensure compliance with the Council's network security policy.

The Contractor will be required to provide specific administration and technical support for the video conferencing service and solution. This will include the provision of a full technical fault resolution service available to schools during school hours.

Test points -
The Contractor should deploy test points and have a testing process that is published on the schools Intranet. These are designed to allow the schools to test key components and functionality of their own components.

- A live test station that will auto answer Incoming calls should be available for H323 and SIP.
- MCU test conferences should be available at all times.

Design guidance
The network link to each school will be set up in such a way as to ensure that video conferencing sessions get the network resources they require to function but do not "hog" the entire bandwidth.

Although existing usage is low there are many schools that rely on the service. It is a service that is growing and the Contractor should size the service to provide concurrent support for the following within one year of service start up.:

- 50 concurrent H323 conferences.
- 100 concurrent SIP conferences.
- 30 concurrent MCU multiparty

Reporting

The Contractor is required to provide the ability for designated Council staff to monitor usage statistics on–line.

The underlying activity recording and reporting must allow for investigations related to bullying or inappropriate usage to be investigated. Time of Day and IP station calling / receiving must be available to enable further investigation.

Records of all video conferencing sessions must be kept in easily accessible format for thirteen months for instant availability. It must be possible for designated Council staff to interrogate these logs with access to information about client, time of day, IP station calling and receiving.

Monthly reports will be produced to show usage statistics to enable the authority to determine the number of users of the service and popularity of conferencing.

Existing Users
The Council will provide details of the E164 number ranges allocated to Hertfordshire schools and sites for video conferencing end points. The Contractor will manage the allocation and distribution of E164 numbers to Council schools and sites to ensure that each school has an appropriate and unique number for each VC end point.

Learning Platform and Video Conferencing -
The Contractor will make available appropriate technical resources to support the integration and delivery of video conferencing into the Council's "Learning Platform" solution and email solutions.

Option for the Contractor to utilise existing service and equipment

Existing video conferencing equipment is provided and managed by:

Videonations Limited, Unit 20, Edward Court, Altrincham Business Park, Altrincham, Cheshire, WA14 5GL Phone: +44 (0) 845 084 3000 http://www.videonations.com

Equipment is as follows:

Description	No.	Details
Tandberg expressway 1163402	1	5 Calls and 25 Registrations 1U Hardware Platform
Tandberg expressway 116341Y5	1	Additional 5 Calls & 25 Registrations 1.00 2610.00
Tandberg Manage Suite Software	1	Tandberg Management Suite 112160 Software Only Version
Tandberg management Suite	1	Additional 25 Systems
Tandberg VCS	1	10 Calls & 50 Registrations
Premier support 12 months expressway	1	Expressway
Premier support 12 months VCS	1	VCS
Premier support TMS	1	TMS
Dell server 3 yr next day onsite support	1	
Tandberg (Codian) MCU 4210 - Codian 4220 high resolution upgrade	1 1	20 port MCU installed in 2006

The Contractor should indicate whether they would be willing to deploy the existing video conferencing solution either to provide resiliency for their solution offered or as part of their proposed service.

See the appendices for a detailed description of the existing video conferencing service set-up

Network support for Voice Over IP

The proposed network solution must support all industry standard IPT and voice over IP prioritisation and quality assurance protocols and mechanisms.

- Local site (if provided) and wide area network support for tagged traffic - Diffserve marking and translation between these two types of QOS must be provided

- Provide a detailed explanation of the traffic prioritisation and shaping that will be implemented to support voice over IP.

.

- Confirm that the proposed network will support all Nortel handset to handset, handset to system, system to system communications and Nortel SIP and H323 trunking and full signalling stacks.

Facility to host equipment

The council will require the facility to "host" servers and equipment in the core Internet sites as the most effective way of delivering certain types of services for example anti-virus downloads.

The Contractor will provide appropriate accommodation for network and server equipment, an appropriate environment (resilient power, air conditioning and security), network links to the core schools network and access for support purposes for third party Contractors of these services. All equipment will be 19" standard rack mountable. Initial indications show a need for no more than 2 x 19" 40U racks.

The Contractor should provide details of the hosting facilities that you will make available to the Council at each of the core Internet sites. There should be the ability for 1x 40U rack of Council related equipment to be co-located at each core site. The need for the authority to use such space will be agreed during the life of the contract. Charges should be identified for this service on a per rack basis and should include all setup charges and ongoing service charges.

Network support for a CCTV service

The Hertfordshire CCTV Partnership operations centre at Stevenage has a 10 Mbps link into the core of the HGfL to provide security video surveillance to Hertfordshire schools sharing bandwidth over the HGfL infrastructure. Currently 20 schools take the service.
The Contractor will provide a secure network overlay and managed resilient synchronous network link into the Hertfordshire CCTV Partnership operations centre. Initially this will be a 16 Mbps circuit. The surveillance centre will be allowed to access only those schools that are under contract with them and will not be given access to any other network or core services. Suitable firewall solutions, IP Filtering and /or ACLs will be used to ensure only designated video surveillance equipment is accessible by the Partnership.

The Contractor will support the CCTV partnership in its deployment of CCTV services to further sites located on the proposed network.

Network links and equipment used for this service will be included in the service reporting mechanism to allow the Council and the CCTV service supplier to monitor the bandwidth usage for performance and capacity management.

DHCP
Currently there is no use of DHCP relay within the HGfL. However the Network and any deployed CPE equipment must support DHCP Relay.

OPTIONAL SERVICES:

The Council believes that the following services would be of benefit to the schools but cannot at this stage identify the take up rate. The Council would like the Contractor to identify if and how they can provide the following services.

Local cabling support and maintenance (Copper category 5e & fibre optic)

The Contractor will offer an on-site managed service for the design, installation, move, patching and repair of school site structured cabling for those schools that are willing to "buy-in".

This service will include options for the support of voice patching over cat5, basic testing and handset deployment.

This service will be managed and charged as a school level facility and structured around a catalogue with unit charges. Each school should be able to 'buy in' to the service using a simple formula based on number of copper and fibre runs within the campus.

If a school "buys in" to this service then the fault diagnosis and repair of "service affecting" cable faults will be included within the overall charge.

Note: this service will not be applicable to BSF schools.

Catalogue options and charges will be reviewed annually with the Council

Cable upgrades and enhancements will be handled as service changes however the Council's objective is to include within the charging structure a percentage of upgrades across the whole site count. The Contractor should identify how they will incorporate this requirement within their proposal.

School sites services – LAN equipment maintenance and replacement

The Council requires the Contractor to propose an option for a fully managed solution whereby ownership of the schools existing LAN network equipment, including WiFi controllers and access points, would be transferred to the Contractor for the duration of the contract

The Contractor will undertake to:

- maintain up to date documentation on behalf of the school and periodically review performance with technical representatives from the school and/or the Council
- provide a maintenance service, including software upgrades and equipment/performance monitoring.
- replace/upgrade equipment as required for support, capacity or performance reasons.
- replace equipment that is no longer capable of support or falls outside of manufacturers full support

Catalogue options and charges for this service will be reviewed annually with the Council

Optional Service: Centralised backup of school servers

The Contractor will provide and support a secure access to either its own facility or a commercially available remote backup service.

If the Contractor is to provide a centralised network based backup service. Then this must offer schools the ability to transfer data for off-site storage as a backup

repository or as a supplementary store for on-site backups. The service must offer a secure FTP mechanism that sites can manually or automatically use to transfer clear, encrypted, normal or compressed data.

The service must support the use of native Microsoft backup tools and utilities like Xcopy and Robocopy etc. and be capable of backing up SIMS and curriculum data. The solution should be capable of handling 4 TB of data upgradeable to 10 TB.

The supplier will also provide a server and workstation scheduling tool to enable automatic backup and recovery facilities.

Network bandwidth usage should be controlled so any single backup or recovery session does not exceed 100 mbps and the total does not exceed 200 mbps within core hours.

Identity management

The Contractor should provide an option of a resilient Shibboleth® / SAML standards based, open source web single sign-on facility.

The service must provide a federated identity and federated single sign-on attribute exchange framework to enable Schools within the HGfL network overlay to offer services between sites or within partnerships or federations.

The service must allow for users in each site to authenticate to on net (both internal HGFL and external Internet) web based services with a single username and password acting as a federated identity provider to content providers under contract to the Council.

An option of Active Directory synchronisation capacity should also be made available to ensure that School level Username and Passwords are also usable across both the internal network and the Internet.

Public WiFi service

The Contractor should provide an option for a network wide public Wifi service that can be delivered to schools, children's homes and associated sites. The service should either deploy on its own network overlay or use technology to tunnel within an existing overlay.
This service should offer WEP and WPA2 encryption and the ability to scale up to 600 separate site based SSIDs as well as offering HTTP interception and 'Hotel' style limited time personal user name and password authentication services.

Design consultancy

These services are in addition to the Trouble Shooter role and will provide the Council with a technical project based design, consultancy and technical assistance service.

This service will be commissioned through the change mechanism and require the Contractor to work with the Council and schools to address schools requirements at a strategic and tactical level.

Typically this might include:

LAN design - A Service to discuss a school's requirements and to produce a recommendation for a cost effective solution. If the solution includes new equipment there should be options for cost effective ongoing support and maintenance.

Video Conferencing - A Service to review school's requirements and to produce a recommendation for a cost effective solution considering LAN setup and endpoint selection, age and suitability. If the solution includes new equipment there should be options for cost effective ongoing support and maintenance.

Firewall and Security – This is for schools that have a need for a local firewall or has a specific security related issue. The consultancy should help the school meet its requirements while being part of the HGfL community and also adhering to the HGfL security policies and best practices. If the solution includes new equipment there should be a central agreement with the Councils security staff to ensure the solution is acceptable and does not compromise overall design principles and common practices. There should also be options for cost effective ongoing support and maintenance

School LAN Active Directory – This will consist of a design consultancy service that will look at schools requirements and produce a suitable AD design that will enable the use of local filtering and other NW related services requiring a streamlined AD configuration. There should also be options for a setup and configuration service and remote maintenance service.

5. SERVICE MANAGEMENT

Service support centre

The Contractor will provide:

- A UK located service management centre to operate, report on and control network and core service delivery to meet the Council's objectives as described in this document. The overall service will support the Council's aims for educational transformation and as such the Contractor will need to maintain a flexible approach to the delivery, development and support of the service provided to the schools in Hertfordshire. The management centre will develop and maintain a close relationship with the school's staff and the Council's SITSS schools' service desk including representing the service by attendance at seminars, school events and Hertfordshire schools conferences.

- pro-active focus on continuous service improvement by analysis of service desk calls to establish trends, root cause of failures of service, and proactively amend working procedures to reduce the level of calls from service users whilst maintaining service levels;

The service will encompass:

- the provision of a managed service desk that will provide a single point of contact for all service requests by telephone (dedicated 0800 number or similar "free phone" service), web, fax and email and will have a direct relationship with

contacts, at the council's "Schools Service Desk", who will be able to raise "service requests". It will also interact with the other service desks that provide services to the Council and the public supporting the current and future needs of the Council.

- the provision of a dedicated service centre manager and technical manager.
- provision of efficient and effective end to end problem, change and service function covering the network and related services.
- the adoption of a proactive and responsive approach which assists the Council in the achievement of its business objectives
- the provision of an end to end installation service for network services covering the complete service from ordering to the installation of circuit, CPE and other equipment. Liaison with school and other site staff, BSF staff and council staff as necessary.
- the operational management of nominated third party suppliers.
- The provision of project services as required by the Council to develop the ICT Infrastructure and integrate third party products
- the provision of operational management of network fault restoration
- management of product and service rollouts
- service "trouble shooter" to provide assistance to schools in cases where performance issues are, in the view of the Contractor, caused by issues within the School IT or LAN environment rather than with the connectivity service itself. This service will include site investigation and consultative visits.

The Contractor:

- will adopt a culture of continuous improvement throughout the life of the contract to further improve quality and reduce unit costs
- will enable the Council to flex its IT network service requirement without exposure to disproportionate fixed charging elements or penalties
- will provide the required skills to implement and exploit advancements in technology, drawing on their experience of the marketplace to be pro-active in identifying, investigating and recommending new technology and solutions which will deliver demonstrable service benefits to the Council
- will proactively participate in service take on activities that are handed over from the Council and/or other Council suppliers as and when engaged by the Council.
- will work within the Council's policies and procedures.
- will not restrict the development of the network or services required within the wider user base due to adherence to a sole technology manufacturer or supplier.
- will apply project management methodology and documentation to all upgrades and roll-outs.
- will operate in line with industry recognised best practice frameworks.
- provide the Council with up to date copies of network diagrams. The details of the content, structure and frequency of updates to be agreed with the Council.
- provide on-line and hard copy access to all information pertaining to the service.
- provide and maintain a dedicated "service catalogue" of all network and core services (including detailed diagrams where appropriate). See the appendices for a copy of the current "HGfL Service Catalogue" as an example of the council's requirements .

- asset management. The Council will require on-line access to the Contractor's asset system (database) and the ability to extract pre-defined and adhoc reports.
- will operate a knowledge base system based on Wiki technology accessible to the Contractor, the Council and user base. This knowledge base will contain documents covering all procedures, design standards, manuals and training materials.
- the Contractor shall implement appropriate systems, processes and procedures to provide for a viable but degraded service desk to be provided in the event of a disaster recovery situation with full service management being restored within 24 hours of the event.

Incident and problem management

The Contractor will provide an incident and problem management service for all users of the various networks and associated services. Some of the more important elements of this service are identified below:

- problem/call management and resolution via a local service desk
- contractor call logging and reporting, incident logging, management and reporting systems made available with full visibility to the Council
- proactive fault diagnosis, identification and fix;
- continuous monitoring and reporting on the status, availability and performance of all equipment (hardware devices and software) used to deliver network and core services including systems to pro-actively identify and report on all fault or exception events and where appropriate automatically raising "incident/trouble" tickets.
- classify all reported incidents and service requests into as many categories as the Council requires.
- automatic establishment of an incident team for issues effecting more than two schools/sites once the problem/incident exceeds the initial SLA parameters.
- advice and guidance to users via the Council's schools service desk
- problem Management analysis including RCA (ITIL) of repeated incidents and related incidents in order to determine the root cause and permanent solution
- change Management and administration (including account administration;
- service requests (e.g. additions, installations and removals of services and assets);
- software and Hardware Configuration and Installation details in the form of a Configuration Management Database (CMDB), Definitive Software Library (DSL) and Definitive Hardware Store (DHS)
- third Party liaison, management and co-ordination.
- proactive management and recording of incidents and problems.
- root cause analysis provided to the Council for all issues involving the incident team.

HCC Schools IT Systems Support (SITSS) service desk

The HCC SITSS service desk will be providing 1st level support to the schools for the services contracted for in this tender and therefore the Contractor will need to work closely with the SITSS service.

The Contractor will need to provide a helpdesk to helpdesk call handling and fault transfer protocol as part of there return. This will be reviewed by the Council and negotiations will take place if required to agree a mutually acceptable inter-working protocol.

Business continuity planning and disaster recovery

The Contractor will:

- provide support to the Council with the on-going development of their business continuity planning process and provide agreed levels of support to the Council when they are dealing with major incidents that involve the invocation of the Council's "Business Continuity" processes.
- attend BCP planning and design meetings and carry out an annual BCP/DR test and desktop review with HCC ICT representatives.

On-site engineering support (trouble-shooter)

The Contractor will provide the Council with the services of an appropriately skilled technical resource to help resolve school service issues where the reason for the problem is unclear i.e. HGfL service or school network.

To lead in the diagnosis of problems the technical resource will need to understand the way in which the Contractor's services are supplied to the demarcation point and also how the school LANs and LAN switch technology operates to provide services to the desktop. This will include knowledge of network and Microsoft file and print Active Directory design and configuration services.

This person will also be required to attend meetings, where necessary together with a Council representative and possibly a third party network support service Contractor. Such site meetings will be called from time to time where there are protracted problems or where the cause of a problem is in dispute.

The Council will use the change control process to request this service, giving 3 working days notice.

Service changes

The Contractor will agree with the Council a fast and efficient stream-lined process that will be aimed at providing a "standard approach" to the implementation of service changes. This will include a structure of pre-defined processes for categorising and implementing service change requests. The Contractor will co-ordinate all changes to services delivered under the contract within the times and service levels identified under the contract

Process for change requests including new services

Change requests will usually be initiated by the Council and will usually involve routine additions, deletions or alterations to particular services at particular sites. The Council may also from time to time request new services for some or all of its sites. Other contract changes may be proposed by the Contractor possibly as a result of a root cause analysis report or other investigative work following a service failure.

The Contractor will –

- provide the Council with a "service change request" form (design to be agreed with the Council and preferably on-line) to use when requesting a service change. The Contractor will only accept a request if signed by an authorised Council representative or received from an authorised representative's email address
- record and categorise (simple, routine or complex,) change requests on receipt of a request form and issue the Council with a unique reference within half a working day

Simple change requests will be completed within one day of receipt.

Routine change requests will completed within two working days of receipt.

For **complex** change requests the Contractor will, within three working days of receipt seek from the Council any further information or clarification that might reasonably be required and within 15 days of receipt of that provide the Council with:

- a written explanation complete with network and/or systems diagrams of the change covering all technical implications and service issues
- any relevant issues and risks
- any implications with regard to the contract
- lead time for implementing the change
- the proposed charge for implementing the change

After initial investigations the Contractor may re-categorise a complex change as **very complex** in which case the completion time must be agreed with the Council within 20 days of receipt of the original change request.

For simple and routine changes the Council will not usually require further documentation prior to implementation. For complex and very complex changes the Council will require documentary evidence, possibly through the production of a Change Notification Form, that the Contractor has operated an internal engineering change control system and employed suitable ITIL style processes to ensure all engineering changes are authorised by a network/service design authority, operational and technical managers. For all such changes the Council's technical sign off of all elements of the change, implementation and back out plan must be sought before the change can proceed.

The Contractor will also provide a mechanism to implement "emergency" service change requests

Change requests and the progress reports will be reviewed at the two weekly operations meetings and monthly account meetings.

Engineering change request service

The Contractor must operate an internal engineering change control system and employ suitable ITIL style processes to ensure all engineering changes are authorised by a network/service design authority, operational and technical managers. Service changes classified as complex will result in engineering changes. In these cases the council's technical sign off of all elements of the change, implementation and back out plan must also be sought before the change can proceed.
At the beginning of each calendar year the Contractor will agree with the Council a schedule of maintenance weekends to undertake service effecting maintenance.

These must be coordinated with the Council's Service desks via the Council service delivery manager. Network maintenance activity must be coordinated with other ICT changes to void conflict and excessive down time or shut down periods.

Best value

The council has an ongoing obligation to provide best value for all of its contracted services. All areas of this contract will be subject to benchmarking and comparison to the market to ensure ongoing best value.

The Contractor will co-operate with the Council in the production and supply of any relevant information necessary to support this process.

If any service request results in a charge to the Council for new/additional equipment then the Contractor will give the Council full details of any equipment so that they can independently test the market.

If the Council can prove that it is possible to source the same/identical equipment with appropriate warranties at a cost that is at least 2.5% lower than that quoted the Contractor will revise its costs in line with the Council's figures.

Preventative maintenance

Preventative Maintenance is defined as "activities that will prevent user problems, system, network, or infrastructure loss or failure".

This element of the managed service is defined within the following activities:

- disaster recovery and backup service;
- a programme of preventative maintenance tasks for all core points of presence and exchange sites
- server/equipment performance and capacity monitoring and management;
- security monitoring and management
- monitoring the performance of key infrastructure and services.
- production of monthly statistics and service maintenance recommendations for discussion at the account meeting.
- maintenance of all hardware in line with the manufacturer's guidance ensuring that no equipment is obsolete or falls outside manufacturers full support unless specifically agreed, in writing, with the Council.
- maintenance of all software in line with the manufacturer's guidance ensuring that no software is obsolete or falls outside manufacturers full support unless specifically agreed, in writing, with the Council.

The Contractor will grant authorised Council personnel full access to all tools used to manage Councils services.

Continuous improvement service

The continuous improvement service is defined as "changes that improve the quality of the service, reduce costs and improve the users perception of the service; ease of use or speed of delivery of requested core and additional services. This will be focused activity to reduce the number of calls in a particular area. It will improve the service to users by reducing faults, making corrections and enhancements quicker or safer to apply, or improving the service in any other way.

The Contractor will undertake a specified work stream/activity associated with the improvement service. Any tasks resulting from the monitoring activity will be undertaken as separate projects and agreed and authorised by the Council prior to commencement.

Statistics and pro-active reporting are required in this area. Statistics will include:

- calls by category.
- reoccurring issues.
- monthly management reports identifying ongoing, re-occurring and large volume issues.

Any costs for the proposals will be reviewed at the two weekly operations meetings. The Council reserves the right to accept, defer or decline the proposals offered by the Contractor.

Adaptive maintenance service

The Contractor will undertake impact analysis, maintenance and testing of the supported service and applications resulting from upgrades of software patches or base application packages or environmental changes.

These tasks, carried out in line with agreed change control processes, will be agreed and authorised by the Council prior to commencement. They will be scheduled and undertaken in the same way as preventative maintenance.

Service hours

The Contractor will provide service as defined below

Network and core services

These services will be available 24 hours a day seven days a week including Bank Holidays.

Network and service support centre

This staffed facility will be available 24 hours a day seven days a week including Bank Holidays to monitor the status of the network and core services and initiate recovery procedures to correct any service effecting incidents.

This facility will also be available to receive calls at any time from a limited number of nominated Council and contract staff where necessary to report and progress incidents or service effecting situations.

Service Desk

The Contractor will provide a fully staffed service desk providing second line technical support, instigation of 3rd party resolution, and where necessary schedule engineers to fix. The staffed service desk will be responsible for the continuation and progressing of calls logged out of supported hours and seeing these through to agreed resolution.

The service desk will be available for the following hours.

Service hours-

Monday – Friday 08:00 – 20:00 (all sites)

Saturday 09:00-16:00 (mainly corporate services)

Sunday 09:00-16:00 excluding Bank Holidays (mainly corporate services)

Network service engineers and engineers involved in the support of site services will be available for site visits Monday to Friday between the hours of 08:00 to 17:00.

Operations Meetings

The two weekly operations meetings are fundamental to maintaining and improving the services. The Contractor will be responsible for arranging these meetings, the venue and the production of agenda, minutes and action lists etc. The Contractor will be represented by the as a minimum the service manager and relevant technical staff.

These meetings will include representation from the Council's first line help desk.

These meetings, chaired by the Contractor are detailed review and planning meetings for the service. There will be a formal format to include:

- previous minutes and actions;
- service review for previous two weeks prepared by the Contractor and the Council's first line support desk and trends from service measures;
- review operational achievements and issues;
- review of current main problem areas;
- review of Operational Service Improvement process and deliverables
- joint prioritisation of the Selected Supplier service improvement activities;
- review impact of changes in service during the previous period;
- review of service changes;
- review of the Risk Management Plan.

Account Review Meetings

The Council will be responsible for arranging this meeting, venue and the production of minutes and action lists. The Contractor will be represented by the named Contract Manager, Customer Service Manager and the relevant service and technical staff. The Council's SITTS schools service desk representatives will also attend these meetings.

These monthly meetings, chaired by the Council's ICT representative are high level review and planning meetings for the service. There will be a formal format to include:

- previous minutes and actions;
- service review for previous month and monthly trends from service measures;
- results of Customer Satisfaction monitoring;
- review operational achievements and issues;
- review of current main problem areas;
- review of Operational Service Improvement process and deliverables
- joint prioritisation of the Selected Supplier service improvement activities;
- review impact of changes in service during the previous month;

- forthcoming changes in the Council business or ICT services;
- review of the Risk Management Plan.
- review financial arrangements and deal with any Service credits.
- annual review of catalogue items and charges

Adhoc meetings

From time to time it may be necessary for the Council to request an adhoc meeting or meetings to discuss matters arising from any area of the contract. The Contractor should attend these meetings and bring the necessary levels of representation to cover the areas to be discussed.

Escalation procedure

The Council require an escalation mechanism and process to raise the profile of service issues within the Contractors organisation.

The Contractor will provide a suitable escalation process for the Council to review, revise and agree as part of the contract.

The process should contain the following touch points:

Contractor's authorised representative interface with HCC Contract Manager
Account Manager interface with HCC Contracting Officer
Managing Director interface with HCC Chief Officer

The process should also:

Provide all those involved in service, account and contract management process with notice of all escalation issues raised.
Maintain a log for review at Contract Meetings of all escalation issues throughout the life time of the contract.

In addition there must be the provision for service credits to be paid to the Council promptly and in the form of a company cheque.

Finances and invoicing

For invoice and financial queries the Contractor will provide the Council with a suitably empowered and named contact available from 09:00 to 17:00 Monday to Friday. Provide their telephone number/s and email address/es.

Invoicing queries raised by the Council will be resolved within one month of them being raised.

Invoices will be presented at the monthly Account Meeting to include any base charges and charges for service changes delivered by the end of the previous month (i.e. at the May Account Meeting invoices to include all charges for service changes completed during April).

All invoices should contain suitably detailed information to enable the Council to deal with them correctly first time. Invoices for circuits must contain A and B end addresses and a full description of the service delivered. Failure to do so may lead to delay in payment for which the Council will incur no financial penalty or loss of service.

Security

The Council take network and information security extremely seriously and will expect the Contractor to do the same. The Council will provide security policy documents and insist that all service offerings are delivered in an agreed secure fashion.

The Council's views in all areas of security will be final although the council will work with the Contractor to agree all solutions.

The Council will undertake regular security audits announced and unannounced, penetration tests and design reviews. Contractor involvement and co-operation will be required. Failure to comply with the Council's policies, standards or agreed security configurations and operational procedures will be viewed as a serious breach of contract. All network and associated services security issues will be rectified at the Contractors cost and dependent on the severity may result in early termination of the contract.

5. SERVICE TRANSITION

Introduction

The Contractor will work with the contractors of the existing service and the Council to ensure a smooth transition of all services and users to the new service without disruption to normal services.

To achieve this they will undertake all design and planning and project management activities required to ensure a smooth transition.

Timescales

The Contractor will provide full services to all schools and related educational sites, as identified in this specification, by the 28th February 2011.

Project Plan and Risk assessment

The Contractor will provide a detailed project plan detailing the process they will use to transfer the existing schools services to the new infrastructure and core services without interruption to the day to day operation of the schools.

The Contractor will provide a detailed risk assessment of the process they propose to use to transfer school services to the new infrastructure.

These two documents will be submitted with the tender response.

The successful Contractor will produce the definitive version of these two documents within one calendar month of the award of the contract. These documents will be used to establish the dates for migration targets to be used to monitor service delivery targets.

The Contractor will provide an online service catalogue during the lifetime of the contract. This will be available within 1 month of contract commencement and will be maintained and updated throughout the life of the contract.

The Council and the Contractor will agree the key milestones identified in the definitive version of the project plan.

The Council will agree financial penalties with the Contractor for failure to meet key milestones. Further information will be found in the Service Level Agreement.

The Council is expecting the Contractor to assign a dedicated Project Manager and implementation team to handle the Service transition.

Service Transition

Service Transition will include but not be limited to the following-:

- the Contractor will be required to obtain the Council's agreement (technical and commercial) in advance for all of its transition plans and programmes.
- initial and ongoing technical design reviews with the Council.
- weekly technical progress meetings with the Council during the implementation.
- bi Weekly Project Review Meetings with the Council during implementation and the initial 2 month period of running.
- as a minimum monthly contract and high level progress review meetings with the Council starting at the signing of the contract and continuing throughout the implementation phase.
- documentation standards agreed in advance covering terms of content, sign-off and timings.
- the Contractor will develop and provide transition information and training as appropriate. This will in some cases include awareness training sessions with support documentation for the support staff and third party organisations working on IT services provided to schools to ensure a trouble free transfer of their services.
- develop and agree with the Council standards/processes for inter-working with our other contractors.
- it will be incumbent on the Contractor to ensure that all parties work together, this will include but not be limited to NTL (existing contractor), BT, the Council's ICT staff, and SITSS

Wayleaves
The Contractor will be responsible for applying for wayleaves and getting works approval from the landlord. All fees will be covered by the Contractor.

Difficult to connect schools
The Council have had considerable difficulty in circuit installations and upgrades to the following sites (see following).

The Contractor will prioritise these sites and be required to provide the Council with a named project manager and a project plan demonstrating how they will ensure these sites receive an appropriate network service by the end of February 2011. A report on progress will be required at every project meeting.

School Name	Address 1	Address 2	Postcode	Phone Number
Anstey First School	Anstey	Buntingford	SG9 OBY	01763 848346
Ardeley St Lawrence CE VA Primary Sch.	Ardeley	Nr Stevenage	SG2 7AJ	01438 861284
Barley First School C of E VC	Church End	Barley	SG8 8JW	01763 848281
Breachwood Green J M I School	Oxford Road	Breachwood Green	SG4 8NP	01438 833115
Forest House Education Support Centre	Harperbury Hospital, Harper Lane	Nr Radlett	WD7 9HQ	01923 427241
Furneux Pelham J M I School	Furneux Pelham	Buntingford	SG9 OLH	01279 777344
Gaddesden Row J M I School	Gaddesden Row	Nr Hemel Hempstead	HP2 6HG	01582 840376
Graveley J M I School	Ashwell Common	Graveley	SG3 6RE	01438 351377
Great Gaddesden C of E Primary School	Great Gaddesden	Nr Hemel Hempstead	HP1 3BT	01442 255734
Hunsdon J M I School	Hunsdon	Ware	SG12 8NT	01279 842644
Jenyns First School	Braughing	Ware	SG11 2QE	01920 821461
Preston J M I School	Back Lane	Preston	SG4 7UJ	01462 451734
Tonwell St Mary's C of E School	Ware Road	Tonwell	SG12 OHN	01920 462894
Wareside C of E JMI School	Wareside, Reeves Green	Ware	SG12 7QR	01920 462354

The Contractor should add any other sites identified during their planning processes as potentially difficult to connect to their network to the above list.

Communication with Schools

The Council will work with the Contractor to facilitate the co-operation of schools in the transition however it will be the Contractor's responsibility to ensure that schools are given adequate notice about what they will be required to do. The Contractor will be responsible for arranging site visits and getting schools compliance. Communication with schools particularly the small ones can be difficult as staff cannot always respond immediately. Please note in some cases this will involve the Contractor's project management staff in site visits and regular contact with schools to ensure they are ready for engineer's visits.

The Contractor will prepare and deliver a change awareness programme aimed at informing the schools of the proposed change, providing detailed “help” via a variety of methods to enable schools to painlessly migrate their services from the existing managed service to the new service.

This may include short awareness sessions for school administrative, technical staff and contractors both in and outside normal school hours. As well as content /pages for the Hertfordshire schools Intranet and email campaigns

The programme will be prepared in consultation with the Council.

School site environment and preparation

The Contractor should note and confirm in the transition plan that they cannot assume that there will be additional power points available within school sites for the new services and that the transition plan should explain how the services will be migrated using existing power points.

The Contractor should visit all schools to carry out a basic survey, identifying power and cabling requirements. The survey should result in a basic line diagram of:

- service intake location
- service type and provider
- any proposed ‘Civils’
- any associated way leaves required (managed and funded by the Contractor)
- power supplies available and any upgrades (provided at the Contractor’s Cost)
- cable routes available and any proposed new routes
- equipment location now and after provision

Note:
For Schools supported by the Council’s SITSS service joint surveys will be required.

It will be the Contractor’s responsibility to recover any old equipment from the school, unless the school wishes to retain, and dispose of it in line with EU legislation and the Council’s environmental standards and policies.

It will be the Contractor’s responsibility to agree with and manage the return or disposal of any existing BT or NTL NTU equipment from the school and dispose of these in line with EU legislation and the Council’s environmental standards and policies.

Service acceptance

The Contractor will be responsible for developing an acceptance plan to be agreed by the Council prior to the order being placed and provide resources and equipment to undertake the tests to the Council’s satisfaction.

The Contractor will be responsible for documenting and updating the acceptance plan.

Two copies of the completed acceptance documentation will be supplied to the Council to support payments.

The Contractor should assume that all acceptances testing affecting “live” services will be undertaken outside the Council’s normal working hours.

The Contractor will provide resources and equipment to undertake acceptance tests to the Council’s satisfaction

The Council expects to use the service reporting tools identified within this specification to support and validate acceptance testing.
The Contractor will agree a site service acceptance plan with the Council, which will identify all processes, with acceptable responses, that need to be undertaken at site migration. The nominated customer representative will be required to sign this document to accept the new service.

The Contractor will have a member of their staff present on site for every service transfer to ensure that the full range of services required at that site are operational and provide the level of response agreed under the contract.

Note: a service or site will not be considered operational until all of the online monitoring and reporting for that service or site is fully functional and available to the users and the Council.

Expiration of Contract with NTL:

The Council’s contract with NTL, our existing supplier, specifies that on the expiry of the contract:

- the network routers in schools and other sites used in the existing service will become the property of the Council

- NTL will hand-over, any equipment used solely to deliver the HGfL service to The Council.

- if requested to so do by the Council, NTL will novate all private circuits, irrespective of supplier, used solely for the delivery of the service to the Council at an agreed reasonable cost to be paid to NTL by the Council.

- NTL will assist the Council to transfer the service to either the Council or another service provider. The charges for such work to be reasonable and agreed between the Council and NTL.

- NTL will provide the Council with all information, programs and scripts used by NTL to deliver the service to the Council in an agreed format if such information, programs and scripts are the property of NTL and NTL is under no obligation of confidentiality to any third party in respect of the same.