The Diocese of Norwich Education and Academies Trust

ICT Services

Framework Specification

Section 2 Table of Contents

3.1 Background

The Diocese of Norwich Education and Academies Trust (DNEAT) is a multi-academy Trust, based in Norfolk and North-East Suffolk who are rapidly expanding as an Academy sponsor and employer. The Trust currently has 30 academies across Norfolk and Suffolk. The specification for the Framework of ICT Services is designed to meet the needs of all DNEAT Academies and Trust offices, should they choose to call off any of the framework of services offered under this contract.

Within this document we will use the following terms to describe the relevant contract stakeholders:

- '**Customer**' – The Diocese of Norwich Education and Academies Trust & all Academies within the Trust or associated with the Diocese of Norwich.
- '**Recipient**' – Any DNEAT Academy buying into any element of the service during the term of the contract. Future Academies that join the Trust during the term of this contract may also be classed as Recipients.
- '**Initial Recipient**' - The Initial Diocese of Norwich Education and Academies Trust recipients that are agreeing to buy into a service
- **'Customer's Representative'** – the nominated single representative from within the Trust who acts as a point of escalation for both the Recipient and the Contractor
- '**Recipient's Representative'** – the nominated single point of contact with contract management responsibility from within a Recipient organisation

At the point of tender, a number of DNEAT Academies are in need of an ICT Managed Service as their existing services are unaffordable, are no longer meeting their needs, or are nearing end of term. We will therefore use the needs of this group of DNEAT Academies (the 'Initial Recipients') to form the initial instruction against the framework.

The Initial Recipients are made up of 9 primary Academies seeking full managed services. Each Academy is at a different stage of development with regards to their use of ICT. These Academies have also demonstrated differing levels of investment made in their solutions which strongly impacts the quality of their current service. Some Academies have had well-funded ICT programmes where others have been underfunded for some time. This range of school types is typical of DNEAT, and the service provider should take note of the breadth of solution quality across the Trust.

Student Numbers	
Initial Recipients	Current Students
Great Witchingham	80
Hockering	48
St Peters Easton	168
Narborough	93
Sporle	78
Castle Acre	64
Bishops	384
Weasenham	33
Rudham	86

Capital Projects: Where the Trust initiates any capitally funded project that is inclusive of any ICT equipment or services, the intention is to enable this contract to be used for the procurement of related ICT goods and services. This Specification is inclusive of all goods and services outlined under the ESFA's ICT specification for capitally funded projects. The Trust would therefore have the option to utilise this contract in agreement with the ESFA through the successful use of an Alternative Procurement Application and could then instruct the Contractor to deliver the capitally funded ICT solution.

3.2 Existing Solution Overview

DNEAT supports its schools through the central procurement of a number of ICT-related Trust-wide services including broadband, HR, Payroll and Financial Management systems. At the time of writing, schools are at different stages in the migration process from their existing services to these contracts. However, during the term of this contract it is expected that all Recipients will be fully migrated onto these Trust-wide contracts.

Information has been provided in Appendix A for each of the Initial recipients including strategic, operational and technical detail (where available) regarding the existing solutions and service provided.

This Section sets out the overall Framework of ICT Services that the Contractor may be required to provide. The Framework is designed to enable the Recipients to select from a menu of goods and services, with relevant options included. Where appropriate, service levels have been specified.

The intention of this Framework is to provide Recipients with the greatest flexibility whilst ensuring best value for money. For example, Recipients may choose to take up options such as: a full managed service, a partial managed service selecting from a menu of service options, third line support, supplementary staffing to cover a Technician for 1 term, or server refresh.

The specific services required by each of the Initial Recipients have been specified in the Pricing Model.

4.1 Overview of the required service options

The Contractor shall provide the following services, for a full description of the below services please refer to Sections 4.2 – 4.8:

a) Operational services, including:

1. Network management
2. File management
3. Storage management
4. Email
5. MIS
6. VLE
7. Finance system
8. Library management system
9. Hosted/ Cloud service administration
10. WAN management
11. Email and Web filtering
12. Remote access
13. Backup and restore
14. Software deployment and updates
15. Security updates/ patching
16. Active Directory services
17. Single Sign-On
18. Server administration
19. Anti-virus
20. Asset management and Auditing
21. Server management
22. Device management
23. Identity management
24. Hardware disposal
25. Disaster Recovery
26. Management of DNEAT.org

b) Support Services, including:

1. Service Desk, to provide support services to users during agreed hours

2. Documentation Services
3. Licence Management
4. Service Requests
5. Capacity Management
6. Third Party Contract Support
7. Supplementary Staffing
8. Regional Resourcing

c) Professional Services - as required, including:

1. Change Services - making changes to the ICT Operational Services in accordance with the provisions of the Agreement.
2. Innovation & Project management
3. Capital Projects
4. Training and CPD
5. ICT Strategic Advice
6. Policy Advice
7. ICT Security Audit
8. GDPR Review (Optional)

d) Contract Management Services – certain actions to enable and assist the Customer to effectively manage the Agreement, including:
   1. Contract Governance
   2. Managed Service Governance
   3. Managed Service Reporting
   4. Contract Reporting
   5. Governance Meetings
   6. Managed Service Handbook
   7. Contract Catalogue
   8. Exit Management

e) Procurement Services – via the Contractor's supply chain, for the purchase of ICT solutions (i.e. equipment and licenses).

f) Service Transfer

g) DNEAT Representative

4.1.1 Hours

The Customer requires support as follows:

Service Hours	Days	Hours	Description
Core Hours	Mon – Fri	07:30 – 18:00	Recipients will individually agree their preferred start time within the range shown for a standard work day. Excludes Bank Holidays and notified Christmas and New Year periods.
Extended Hours Options	Mon - Fri Sat - Sun	06:00 – 22:00 08:00 – 17:00	Can include Telephone support to rectify Remote

			Access issues and/or local support on an as needs basis.

A range of extended hours must be provided as costed options and may include early start, late working and weekend support. Initial Recipients have indicated their required hours within the Pricing Model.

4.1.2 Ownership

The Customer intends to retain ownership of all on-site equipment, cabling, licenses and data.

The Customer's assets are available for the Contractor to use to deliver services to the Customer.

The Customer is open to proposals for innovation in the delivery of the service. Relocation of systems or alternative approaches to delivery of the service will be considered.

As part of the service described subsequently, the Contractor shall recommend an equipment refresh model to the Recipients for budgetary planning.

4.2 Operational Service

Recipients may choose to take up the following services as part of a full or hybrid managed service. Where relevant, recipients may choose relevant elements of support on a 2nd/ 3rd line basis.

4.2.1 Network management

The Contractor is to manage, operate and maintain the Customer's data network in accordance with agreed service levels to support the service, in addition to any other requirements that the Customer may have. This shall include, but may not be limited to:

- Maintaining any existing network infrastructure including all active network equipment, e.g. switches, wireless controllers, access points, routers, firewalls, etc.
- Supporting the components needed to provide the network connectivity and bandwidth required to meet the Customer's requirements
- To maintain and operate the network to meet the Customer's requirements
- To manage wide area communications services via 3rd party suppliers in the way that provides best value for the Customer
- To represent the Customer in third party supplier user engagements to support any roadmap planning

The Contractor will provision, operate and support the data network, including traffic and bandwidth management.

The Contractor shall undertake proactive monitoring of the active network to identify potential problems at an early stage. The Contractor shall install any software and firmware updates in line with equipment manufacturers recommendations.

The Customer requires that the network is maintained with no single point of failure throughout the network, unless otherwise agreed by the Recipient. The Contractor is required to maintain the network to provide the availability, capacity and resilience required to deliver the ICT Service. Where the network is under-performing, the Contractor shall advise the Customer with options to improve the service.

Where a Recipient's solution includes on-premise systems that run over the IP infrastructure, the Contractor is required to ensure there is sufficient capacity and availability on the network to operate such systems. Examples include, but are not limited to: building management systems (BMS), CCTV, access control, biometric or Smartcard identity systems, telephone systems, multi-function print/copy devices.

The availability requirements are set out in the KPIs.

4.2.2 File Management

The Trust requires the Contractor to support a fully configured file service. This shall include, but may not be limited to:

- Provision of sufficient file storage, sized in accordance with Customer requirements.
- Setting of access rights and permissions
- Setting of quotas based upon user groups
- Reporting to the Customer to inform decisions regarding expansion, where required.

4.2.3 Storage Management

The Customer requires that the storage is maintained at an agreed capacity. The storage solution will be used for both user storage and shared areas and should maintain sufficient capacity to support growth in the volume of stored data.

Storage quotas will be managed to the parameters set by the Customer.

Data to be stored and handled in accordance to any current legislation, including legislation that is not yet in place at the time of tender but that becomes a requirement during the term of the contract. For example, personal data covered by the Data Protection Act 1998, any credit or debit card information to be processed and managed according to the Payment Card Industry Data Security Standards (PCI DSS). Data that is stored in cloud or hosted systems should be held in UK based datacentres.

4.2.4 Email

A service is required to operate and maintain the Customer's email solutions. This includes, but is not limited to, setting up new users, deleting users, setting up user groups, backing up user email accounts and messages, restoring user e-mail accounts and messages, and email archiving. Recipient solutions may include on premise, hosted or cloud-based solutions.

4.2.5 MIS

The Recipients use a range of MIS products including on premise, hosted or cloud-based solutions. The Contractor is required to manage and maintain the MIS hardware and software infrastructure (including software upgrades) in accordance with agreed service levels.

The Contractor may be required to interface with third party MIS providers where solutions run on the IP infrastructure and/or where they integrate with active directory.

4.2.6 VLE

A range of online tools and VLE products may be in use by Recipients. The Contractor is required to maintain each solution in accordance with agreed service levels.

This requirement may also include optional support for configuration. Should the Customer require new functionality, the Contractor (via Service Request) would be expected to deliver this functionality.

4.2.7 Finance Systems

Finance functions for the majority of Recipients are currently supported through the use of PS Financials, a centrally procured product that is accessed via RD session.

Availability requirements are set out in the KPIs.

4.2.8 Library Management System

Library management is supported through products individual to each Recipient and include on premise, hosted and cloud-based solutions.

The requirement is to manage and maintain the hardware and software infrastructure required for the delivery of each library management service in accordance with agreed service levels.

The Contractor may be required to interface with third party LMS providers where solutions run on the IP infrastructure and/or where they integrate with active directory.

4.2.9 Hosted/ Cloud System Administration

The Contractor will deliver the system administrator function for hosted/ cloud services (e.g. O365, Google for Education, MS Azure for storage, MS Azure active directory).

4.2.10 WAN Management

Broadband services are currently provided by a range of service providers. It is expected that all Recipients will migrate onto the Trust-wide broadband contract (currently with Updata) during the term of this contract. The requirement is to manage the interface between the Customer and the broadband provider. This includes ensuring that the capacity continues to meet the Customer's requirements.

4.2.11 Email and Web Filtering

Email filtering and web filtering are currently provided by a range of solutions/service providers. It is expected that all Recipients will migrate onto a Trust-wide eSafety contract (to be sourced) during the term of this contract. The requirement is to manage the interface between the Customer and their filtering provider and to provide system administration for the filtering solution in accordance with agreed service levels.

The service must ensure that the solution is configured in manner consistent with the Customer's responsibilities for safeguarding.

4.2.12 Remote Access

Remote access shall be provided to applications and services as appropriate to the Recipient solution. For the purposes of this specification remote access means access to the Recipient's applications and services from a location that is not directly connected to the main Customer network infrastructure. The Contractor is required to maintain and monitor the current solution and to ensure that capacity continues to meet Customer requirements. The Contractor shall monitor risks and advise on the suitability of the solution (i.e. to address risks identified due to changes in security).

Recipient email systems should be made available, where applicable, for remote access using an appropriate method, e.g. browser based web-mail, smartphone/tablet app, etc

4.2.13 Backup and Restore

All Recipient servers, systems, applications and user data will be backed-up and retained to an agreed period of time. Data includes, but is not limited to all data, including email, held on all servers and storage devices (e.g. SAN, NAS, etc.) whether on-premise, hosted or cloud-based.

An appropriate GDPR compliant backup regime to be agreed with each Recipient which includes frequency and type of backup for servers, systems, applications and data. This should include clear Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for each Recipient.

A backup retention period will be agreed with each Recipient and adhered to. Restores are required for each type of data. For user data this will be to the file level. For e-mails this will be to each user account level.

Backup sets should be held remotely from the Recipient's server room environment, to allow for the full recovery of the Recipient's servers, applications and data in the event of any

disaster recovery scenario including the loss of the Recipient's main site. The Contractor will assist any Recipient experiencing loss of service due to disaster, in recovering servers, system, applications and data in line with Recovery Time Objectives.

The Contractor should conduct, as a minimum, annual testing of the Recipient's disaster recovery plan, including testing full restore of servers, systems, applications, and data to ensure a recovery is achievable within the scope of the plan and based on recovery point objectives and recovery time objectives.

The Contractor must recover any lost data requested by users within an agreed period of time, which is detailed within the KPI section of the specification.

The Contractor shall advise the Customer on best practice for secure storage of back up media, agree the process and adhere to the agreed process.

Recipient data stored in any systems or files, managed, administered or accessed by the Contractor are the property of the respective Recipient.

4.2.14 Software Deployment and Updates

The deployment of all new software and associated updates will be the responsibility of the Contractor. The scope of the service includes all software currently on the Customer Software List and those added to the list via change control.

4.2.15 Security Updates and Patches

The network shall be protected from unauthorised access. Updates to the tools used to provide this service shall be applied as soon as practicable after release, and evaluated by the Contractor for any impact on the Recipient's environment. Deployment of updates should not interfere with the running of the school, e.g. lessons and should be communicated to the Recipient if the deployment is likely to cause any downtime or reduction of service.

4.2.16 Active Directory Services

The Contractor will maintain the AD structure to best practice standards.

The Contractor will ensure that group policies are appropriate to support teaching and learning whilst maintaining a secure and safe environment for students and school data.

4.2.17 Single Sign-On

The Contractor will maintain and manage the Recipient's single sign-on solution in accordance with service levels set out in this document.

4.2.18 Server Administration

The Contractor shall maintain and support the server environment in accordance with agreed service levels. This may include direct attached storage, network attached storage or storage area networks. This shall include but may not be limited to:

- preventative maintenance activities, including patching
- software and firmware upgrades

- corrective maintenance, i.e. returning the equipment to operating in accordance with the manufacturers' specifications
- configuration management of the hardware

4.2.19 Anti-virus

The Customer requires that all servers/computers connected to the network will be monitored on an ongoing basis for potentially harmful programs and viruses. Weekly scans will take place on a scheduled basis during periods of low usage. All portable media will be scanned upon connection to the network before access to their contents is granted to users. The anti-virus solution must be checked daily for failed device installations and failed updates.

4.2.20 Asset Management and Audit

The Contractor is required to maintain Asset Lists of all ICT equipment.

ICT assets must be labelled with suitable secure labels identifying the correct owner of the asset and with a unique asset identification number.

An annual ICT asset audit must be performed. The results of the audit will be used by the Recipient to inform decision making regarding refresh spending. The audit must identify utilisation levels per device.

4.2.21 Server Management

The Customer requires that the servers are maintained (physical and/or virtual).

Availability requirements are set out in the KPIs.

4.2.22 Device Management

The Customer requires that devices are maintained which includes but is not limited to desktop PCs, laptops, tablets and other computing devices. Each Initial Recipient has provided an ICT Asset List itemising their current devices within Appendix A.

Availability requirements are set out in the KPIs.

4.2.23 Identity Management

All users – students, staff, Governors, adult learners, or other nominated individuals – will be managed by the Contractor. This will include, at minimum:

- User provisioning
- Removing users
- Guest access
- Setting user permissions
- Maintaining users within AD
- Resetting Passwords
- Reviewing systems and network usage to ensure adherence to the Acceptable Use Policy.
- Monitoring and controlling storage to ensure adherence to storage limits

User provisioning during annual transition must be treated as an SR3, as detailed under Section 4.4.1.

4.2.24 Application Management

The Contractor shall manage applications, including, but not limited to:

- Provisioning the appropriate infrastructure (server, operating systems, and databases) to support each application
- Providing a central point of contact for the management of application issues
- Managing the interface to the application support provider

It is noted that support for the applications themselves may be provided by others. See Section 4.3.1 - Service Desk for a description of activities required with reference to third parties.

4.2.25 Print Management

Print management is supported through use of a range of print management software products. The requirement is to manage and maintain the hardware and software infrastructure required for the delivery of the print management services as in accordance with agreed service levels.

The Contractor may be required to interface with third party Print Management providers where solutions run on the IP infrastructure and/or where they integrate with local network management utilities (for example Active Directory, Open Directory, etc.).

4.2.26 Printer Management

For devices, such as leased printers, which may be inclusive to a third-party contract, the requirement is to supply network connectivity for these devices and if required, to configure a print queue.

Where devices are not included within a third-party contract, these are included in the Asset List – the Contractor shall maintain these printers as in accordance with agreed service levels.

4.2.27 Hardware Disposal

All hardware disposals will comply with the WEEE directive and its subsequent iterations A data destruction certificate must be provided for each device disposed. All ICT Assets that reach end-of-life will be recorded in the asset management system and their disposal recorded to ensure traceability.

It is expected when disposing of ICT assets, that the Contractor will seek to generate a fair market value for disposal items. This income should be passed onto the Recipient.

4.2.28 Disaster Recovery

In the case of Recipients that have not yet instructed a support service by the Contractor, an emergency call out service shall be provided enabling any Recipient to draw upon technical support to assist the local team in dealing with a major incident (e.g. ransomware attack, local server failure). The nature of the incident and the capacity of the Recipient will determine the

type of support required. Support shall be charged via the Supplementary Staffing rates indicated in subsequent sections.

4.3 Support Services

The Contractor shall use processes based on ITIL best practice.

4.3.1 Service Desk

The Contractor Service Desk shall be the single point of contact for all users for all ICT problems and queries relating to ICT services.

The Contractor Service Desk shall be available during Core Hours to respond to all types of incidents and at all other times to log low priority incidents for response during core hours. At minimum, this will include:

- Unlimited remote support
- A Service Desk that is Trust-oriented
- Enables liaison and tracking of incidents relating to ICT 3rd parties
- 24/7 access to a web-based interface for logging and reviewing incidents
- Self-help knowledge base for staff, accessible via the Service Desk
- Service Desk integration with email, enabling Recipients to log new calls and receive progress updates by email
- Dedicated telephone service, available during hours as specified under Section 4.1.1.
- Real-time tracking of incidents

The Contractor is to maintain a log of all fault or enquiry calls. As a minimum, the log is to contain the following information:

- Unique call reference number
- Details of the person raising the call and the call time
- A description of the fault or enquiry
- The categorisation of the fault or enquiry agreed with the Customer
- Call status and the times at which the status is changed (i.e. the time at which a fault is rectified and the call is closed). Calls shall only be closed with the written agreement of staff affected
- The cause of any fault and actions required to remedy it

If there is a fault in a service supported by a third-party supplier, then the Contractor shall:

- Inform the Customer that there is a fault with a service supported by a third party
- Investigate the technical fault locally prior to escalation to the third party
- Provide any necessary assistance to the third-party supplier to ensure that the affected services are returned to operation as quickly as possible

The Contractor must provide first line support for all third-party suppliers (unless the Recipient wishes to manage the interface directly). Where providing first line support, the Contractor must:

- Contact the third-party supplier on behalf of the Trust to describe the problem and identify the appropriate way forward

- Monitor progress of fault resolution, provide regular progress updates to the Customer and escalate as necessary

All faults, whether or not a third-party supplier is involved, are to be prioritised as defined under Incident Management, Section 6.4.

The performance targets for the resolution of faults are set out in this document.

The Service Desk shall monitor the progress of all fault or enquiry calls to ensure that they are resolved within the agreed timescales.

Feedback shall be provided to the originating user for every call.

As defined within Incident Management Section 6.4, for Priority 1 & 2 faults the Service Desk shall:

- Inform the Customer when the fault is confirmed of the actions being taken to correct it and the time at which the service is expected to be restored
- Update the Customer on the status of the fault and of actions being taken regularly until the full service is restored

For Priority 3 & 4 faults the Service Desk shall:

- Inform the user who reported the fault that actions are being taken to rectify the fault and the time at which the service is expected to be restored
- Update the Customer once the full service is restored

The call log must provide sufficient information to allow accurate monthly reporting of service performance for all the services provided

4.3.2 Documentation services

The Contractor shall maintain documentation describing Recipient systems and procedures used to provide ICT services.

This documentation shall include, for all systems used to provide services to the Trust:

- The location and configuration of the system, including details of the hardware, operating system and any bespoke or packaged software
- Design documentation
- Administration and operating procedures

The documentation will be stored safely and remotely accessible by Recipients and the Customer 24/7. The documentation will remain accessible for 12 weeks after the contract term expires.

4.3.3 Licence Management

The Contractor shall manage all existing licences (and new licenses procured during the term of the contract) that are required for the provision of the ICT Services and shall be responsible for notifying the Recipient when additional licences are required. The Customer and/or Recipient will procure all licenses unless this is specific to a product that the Contractor requires for delivery of the service.

4.3.4 Change Management

The Contractor shall manage the function to identify, review, approve and incorporate change into the Customer's managed service. This will include changes to any service solution, technologies, systems, applications, hardware, software, processes and procedures relating to the ICT service. This shall include creation and maintenance of:

- Documentation detailing changes to any element of the managed ICT solution
- A central definitive software library of all master copies of the software that form the ICT solution

4.3.5 Capacity management

The Contractor shall be responsible for monitoring the use of resources (processor utilisation, memory, disk, bandwidth, etc.) and for advising the Recipient where appropriate steps are needed to prevent any deterioration of the performance of the ICT Services over time. Monthly reports should be generated that capture performance data.

4.3.6 Management of third party contracts

A number of services are currently provided to the Customer by third parties, such as printer/MFD leasing and cashless catering.

The Contractor shall interface with third parties, as needed to meet Customer requirements, where solutions run on the IP infrastructure and/or where they integrate with local network management utilities (for example Active Directory, Open Directory, etc).

The Contractor will be required to interface with third parties as described under Service Desk (i.e. provide assistance to the third party to ensure services are returned to operation)

Where needed, the Contractor shall support the Customer in renegotiating contracts with third parties by providing technical and specification guidance.

4.3.7 Supplementary Staffing

The Contractor shall offer a service to provide supplementary ICT staffing to Recipients.

This staffing service can be used by any Recipient, regardless of their call-off of any other element of the service. For clarity, a Recipient may use this service without purchasing a full managed service. Equally, where a Recipient is procuring a manged service from the Contractor, this Supplementary Staffing service could be used, for example to flexibly 'top up' existing on-site resource. To illustrate, a Recipient may purchase a Tier 1 Managed Service and request the addition of 1 x half-day visit per week by a Junior Technician to support a pilot project over a half-term.

Staff should be suitably qualified in the area where they are being deployed.

The staffing requests may be requested for short-or long-term temporary appointments. The minimum notice period for a short-term temporary appointment will be 48 hours (e.g. to provide sick cover for a Senior Technician employed by a Recipient). The notice period for long-term temporary appointments will be relative to the appointment.

In the case of a major incident occurring at an Academy that is not yet a Recipient of a managed service, the Contractor shall provide an Emergency Call Out service using the Supplementary Staffing Service function. The scope of works and the role required for the

service will be dependent on the requirements to support disaster recovery and will be therefore agreed between the Contractor and the Customer's Representative & Recipient on a case by case basis.

Appointments can be made based on daily rates, or for long-term temporary appointments, can be agreed on a weekly, half-termly, termly, term-time only or annual basis.

A range of roles have been identified as possible appointments under this contract and include:

Project Manager	Project Management resource for implementation of ICT projects, also including SR4 changes and capital projects. Where appropriate, includes resource to liaise with Design & Build Contractor for Recipient school extension/refurbishment or Future Recipient capital projects (Skill expectations – Prince2 or equivalent experience)
IT Manager	IT leadership resource to oversee the delivery of the ICT Service to the Recipient. May include line management responsibility over the Recipient's ICT technical team.
Network Manager	Network management resource to design, deliver, manage and/or support the Recipient's ICT solution, with special emphasis on network infrastructure. May include line management responsibility over junior members of the Recipient's ICT technical team. (Skill expectations – Appropriate qualifications (Computing Degree or applicable professional qualifications such as MCSE) or experience of managing a Microsoft Server environment and associated client devices.)
Senior Technician	Senior technician resource to design, deliver, manage and/or support the Recipient's ICT solution. Includes support in delivery of SR4 changes and capital projects. (Skill expectations – Appropriate qualifications (Computing Degree or applicable professional qualifications such as MCSE) or experience of managing a Microsoft Server environment and associated client devices.))
ICT Technician	ICT technician resource to deliver, and support the Recipient's ICT solution as directed by a senior staff member. Includes support in delivery of SR4 changes and capital projects. (Skill expectations – Appropriate qualifications or experience (ComTIA A+ or equivalent)
Junior IT Support	Entry-level IT support resource, can include apprentices (Skill expectations – Appropriate Experience and Working towards a relevant qualification)
General labour	Resource to decant ICT equipment (excluding any specialist works) from one location to another
AV decant & reinstallation	Specialist AV resource to decant AV equipment and cabling from one location to another, includes safe de-installation and re-installation
New AV installation	Specialist AV resource to install new AV solutions into classrooms
Senior Trainer	Senior Training resource to provide user training services on ICT solutions and ICT best practice in (Skills expectations – training certification in relevant solutions, as appropriate)
Trainer	Training resource to provide user training services on ICT solutions and ICT best practice (Skills expectations – training certification in relevant solutions, as appropriate)
ICT Strategic Advisor	Consultant to advise on ICT strategy, may include educational, technical, operational and commercial strategic advice; May include interim ICT Director posts
ICT Educational Specialist	Consultant to advise on ICT educational best practice, ICT curriculum design, ICT CPD planning, ICT recruitment, ICT in teaching and learning, ICT innovation
Senior Software Engineer	Senior software specialist to specify requirements, to design/customise bespoke products and software integration projects. Includes engagement with third party software providers to configure existing systems and to test and snag implementations. (Skills expectations –

	web based software development, including Java, Visual Basic, web development tools, e.g. Ruby, Python, PHP or similar)
Junior Software Engineer	Junior software specialist to support specification of requirements and software integration projects. Includes engagement with third party software providers to configure existing systems and to test and snag implementations. (Skills expectations – includes Visual Basic, Python, web tools or similar)
Website designer/ developer	Support the design and update of Customer or Recipient website and other web-based services (e.g. apps or bespoke portals). (Skills expectations – website content management systems, wireframes, CSS styling or similar)

Where a Recipient has procured a managed service and an increase of on-site presence is requested by the Recipient, the Contractor must first assess whether the increase can be accommodated within the contract and would not therefore be chargeable (e.g. a single pre-planned high-profile parent event or planned high risk exams period). Suspension of the service levels should be considered, where applicable, see Section 6.7 for details. Where it is determined that the increase exceeds the provision of resource inclusive within delivery of the service, this can be called-off based on additional charges proposed and agreed, based upon the rates included in the contract.

Note that day rates should be based on a standard work day (i.e. 8 hours) and exclusive of travel time.

4.3.8 Regional Resourcing

Delivery of support services via this contract shall allow for the sharing of resource across Recipients.

4.4 Professional Services

4.4.1 Service Requests

There shall be multiple levels of Service Request, with distinct response processes for each, as follows (example Service Requests are non-exhaustive):

- SR1 - Simple changes: changes which have low impact on the existing ICT environment e.g. password reset or revised permissions;
- SR2 - Standard changes: changes which will have an impact on the existing ICT environment e.g. modifications to profiles, data storage or mailbox settings, processing staff leavers and joiners;
- SR3 – Planned Project changes: changes which are expected as part of the annual operational cycle that are time-sensitive and warrant management of the change as a project, e.g. annual transition, new starters, exam results. SR3 Planned Projects are inclusive to the service and will not incur any additional service charges. The purpose of the treatment of these inclusive regular projects is to make explicit to both Customer and Contractor that these activities need to be planned and to assess any impact on business as usual.
    - The Customer requires the Contractor to develop a Programme of Planned Projects, reviewed at each Service Management Meeting in order to plan in advance for pending SR3 changes. This will enable both parties to proactively

prepare for these time-sensitive activities and ensure sufficient resource is made available at these peak times.

- SR4 – New Project changes: changes which are large or complex enough to warrant management of the change as a project such as additions, new functionality, installation of new software components, hardware requests, etc. Depending on the scope of the SR4 New Project, this may be delivered inclusive to the service, or may incur an additional charge.

The Contractor shall acknowledge and respond to all Service Requests in accordance with the KPIs set out in this document.

The Contractor shall be responsible for all configuration management activities relating to Service Requests.

All SR4 requests shall be subject to written confirmation from the Customer to proceed to implementation and such confirmation shall include:

- The agreed completion date and time for the request
- A detailed scope of works for the request including proposed timeline identifying milestones
- The risk and mitigating actions that the Contractor must take
- The costs for implementation
- SLAs agreed individually per Request indicating successful completion (i.e. to time, to quality, to budget)
- User acceptance tests (as appropriate) to measure SLA adherence

It should be noted that where an SR4 request is complex, it may require specialist support by the Contractor to enable the Customer to reach agreement to the SR4 scope of works. In this case, a process has been defined under Innovation (see section 4.4.2).

4.4.2 Innovation Projects and Project Management

The service shall also include at the Customer's request, the delivery of projects requiring support for innovation. Project 0s might address:

- improvements to current functionality that is not meeting requirements to the satisfaction of users
- innovative ICT projects that take the business or the Academy forward
- requirements to refresh or grow a material element of the existing solution

Depending on the size and complexity of the requirement, additional support may be required to assist the Customer in defining the scope of works and in identifying risks and mitigations for the project. This support may be inclusive to regular account management practices or may require specialist activities to be instructed (e.g. detailed design work).

Once the scope of works is agreed (and where this is part of a Managed Service, the SR4 instructed), the works should be delivered as a project with no unplanned disruption to business as usual. A Project Manager should be identified as the point of contact for delivery. The Project Manager will be required to manage the project programme, to report regularly on project progress, and to maintain a risk register specific to the project.

Each project will be reviewed individually between Contractor and Customer to determine which project-specific KPIs should apply and how these will be measured. At minimum, each

project shall be reviewed in terms of delivery to agreed budget, to agreed programme and to agreed quality indicators (i.e. user acceptance tests).

4.4.3 Capital Projects

Where the Customer initiates any capitally funded project for a Recipient or a Future Recipient (e.g. Free School), the Contractor shall at the request of the Customer, provide the ICT-related goods and services specified for delivery of the capital project. Provision may include:

- Supply and delivery of ICT equipment and services (as outlined under Section 4.6)
- Project management, including (where relevant) liaison with Design & Build contractor
- Technical design, integration and installation of the ICT solution
- ICT decant, including (where relevant) specialist audio-visual decant and installation
- Training
- ICT strategic advice, including ICT educational specialist advice

4.4.4 Training and CPD

The Customer wishes to ensure that all staff are confident, competent and effective users of relevant technologies. The Contractor shall provide CPD and user training services for Customer teaching and support staff if requested to do so.

Training and CPD services may include activities such as training need analyses, development of training and/or CPD plans, development of training modules and materials, delivery of training sessions, and evaluation of training. Training and CPD activities will be delivered to suit the needs of the Recipient and may include approaches such as twilight sessions, train-the-trainer models, inset days, away days, distance learning support, online self-help, and mentoring.

Where a Recipient will retain its own technical staff, the Contractor shall provide technical training and technical CPD services, if requested to do so by the Customer. This can include provision of professional development based upon an accredited method.

Where training falls outside the skill sets of its own staff, it is expected that the Contractor will include within its supply chain high quality training partners.

4.4.5 ICT Strategic Advice

The Customer will maintain the development and ownership of its ICT strategy. The Contractor will advise the Customer in development of the strategy, where requested, and will deliver the strategy.

The Contractor will be required to provide strategic advice, at minimum including:

- Input to the Customer's and the Recipient's development of their ICT Strategy
- Advice on refresh cycles on all hardware, including identifying opportunities to make best use of limited resources
- Input to budget setting for new ICT purchases

The Contractor will be required to provide strategic advice specific to the needs of the Customer and individual Recipients. This advice may be provided inclusive to the service, included as part of a sales/account management function, or as a chargeable service. For reference, examples of current topics identified by the Initial Recipients include:

- Advice on new technology developments and adoption
- Advice on technology to support specific areas across the curriculum
- Purchase of refurbished hardware
- Equipment financing and/or Hardware as a Service (HaaS) as a potential alternative method to capital device procurement
- Advice on capital programmes (e.g. school expansion, refurbishment). This may involve advising on ICT provision for temporary buildings, repurposing of rooms, or new buildings.
- Identification of possible funding streams for ICT investment
- Development of 1:1, BYOD and parental contribution programmes

4.4.6 Policy Advice

The Customer will develop and own School Policies. Where required, the Contractor will advise the Customer on the ICT elements of School Policies, and will deliver the ICT elements of each policy. Relevant policies include, but are not limited to:

- ICT elements of the Business Continuity and Disaster Recovery (BCDR) Policy
- Acceptable Use Policy
- eSafety Policy
- Safeguarding Policy
- Data Protection Policy in line with GDPR

4.4.7 ICT Security Audit

The Contractor will perform an audit of Recipient procedures, controls, documents and the management of processes in relation to IT security. At minimum, the audit should include relevant engagement (e.g. site visits, interviews) and documentation review, resulting in a written report outlining the current state, identified risks and recommendations.

4.4.8 GDPR Review (Optional)

The Contractor will perform a service to review Recipient practices and processes in the management of data in line with GDPR. At minimum, the review should include relevant engagement (e.g. site visits, interviews) and documentation review, resulting in a written report outlining the current state, identified risks and recommendations.

4.5 Contract Management

This section defines the relationship between the Customer and the Contractor during the period of the Agreement.

4.5.1 Staff

For each of the staff who will carry out delivery of the service, the Contractor shall ensure their staff are suitably qualified and competent to undertake the work and shall conform to Recipient School Policies while on site. Wherever possible, the Customer urges the Contractor to provide ongoing CPD for its staff. The Customer wishes to participate in the interview process for new appointments, particularly where an individual is being assigned to work a minimum of 0.5FTE on the Recipient site.

Any staff working at the Trust will be required to undergo employee induction for the institution(s).

The Contractor shall ensure all staff have been vetted and comply with DBS requirements.

The Customer must be informed 1-month in advance of any intention to use alternative staff.

4.5.2 Contract Governance

The Contractor shall appoint a Contract Manager who shall govern and manage the contract across the Trust. This role will:

- be responsible for the provision of all ICT Services delivered across the framework
- be contactable by the Customer during core hours
- attend regular meetings at locations and frequencies agreed with the Customer
- attend ad-hoc meetings with the Customer when requested to do so

The Contractor shall identify a senior manager to be the point of escalation for any issues that cannot be resolved by the Contract Manager.

The Contractor shall not replace the Contract Manager or the Senior Manager during the contract without the Customer's written agreement to the proposed replacements.

4.5.3 Managed Service Governance

As this framework includes the option to call off managed services, there is a requirement where one or more Recipients take up a form of managed service via this contract, for the Contractor to appoint a Service Manager who shall:

- be responsible for the provision of the ICT managed service(s) to Recipients via this contract
- be contactable by the Customer during core hours
- attend regular meetings at locations and frequencies agreed with the Customer, see section 4.5.6 for further information
- attend ad-hoc meetings with the Customer when requested to do so

The Contract Governance and Managed Service Governance functions are distinct in their responsibilities, but may be delivered by a single role, if appropriate. The Contractor shall identify a senior manager to be the point of escalation for any issues that cannot be resolved by the Service Manager.

The Contractor shall not replace the Service Manager or the Senior Manager during the contract without the Customer's written agreement to the proposed replacements.

Should the account grow to include a greater number of managed service Recipients, the Customer may develop an ICT Governance Group to inform the ongoing improvement of the service. The Group would be made up of nominated Recipient Representatives and would be led by the Customer’s Representative. The Contractor would be required to provide representation to the Group via the Service Manager and Contract Manager (where appropriate).

4.5.4 Managed Service Reporting

The Contractor is to provide a Service Report to each Recipient at an agreed frequency (e.g. monthly) which provides the information required to assess the quality of the services provided and identifies any areas of concern.

The format of the Service Report will be agreed with the Recipient, and should include the following types of information:

- Details of performance against the SLAs and KPIs
- Explanation of the reasons for any failure to achieve target performance levels, together with description of any steps being taken to avoid any problems recurring
- A summary of incidents in the reporting period
- A summary of capacity, fault, performance and any other relevant trends, together with recommendations as to any necessary actions to maintain or improve service levels
- Details of any proposed plans for planned maintenance and the way in which any consequent service disruption will be minimized
- An annex summarizing all Service Desk calls received in the reporting period

The Contractor is to provide a Trust Quarterly Managed Service Report for use by the Customer's Representative which summarises information across all active managed service Recipients in a single report. The purpose of the report is to assess the quality of the services provided across all Customer Recipients.

4.5.5 Contract Management Reporting

The Contractor is to provide a Trust Quarterly Contract Report for use by the Customer's Representative which summarises information across all orders placed, projects delivered (or in progress) and services in delivery under this contract in a single report. The purpose of the report is to assess risks and opportunities regarding the delivery of goods and services via the contract. The purpose is also to assess the quality of that delivery. The report shall include information regarding any element called off the Framework by any Recipient. The content and format of this report will be agreed between Contractor and Customer on appointment.

4.5.6 Governance Meetings

The Contractor's Contract Manager and/or Service Manager, and other Contractor staff as deemed appropriate by the Customer, shall attend relevant meetings including:

- Managed Service Management Meetings for each Recipient at agreed frequency (e.g. termly): at which the performance of the Contractor up to the previous quarter shall be discussed and any issues or risks addressed, together with any other agenda items identified by the Contractor or the Customer;
- Contract Management Meetings at agreed frequency (e.g. termly) at which the performance of the Contract-at-large shall be discussed and any issues and risks addressed, together with other agenda items identified by the Contractor or the Customer;
- Other meetings as requested by the Customer's Representative or the Recipient's Representative, including reviews with senior leaders, workshops with users and third-party suppliers to discuss service improvements, internal meetings and committee meetings.

4.5.7 Managed Service Handbook

The Contractor shall publish and maintain a managed service handbook that includes:

- Contact details for the Contractor and Customer key parties
- Details of the service provided
- Details of the support provided

- Details of third party services managed by the Contractor
- Change process
- Roles and Responsibilities
- Escalation procedure

4.5.8 Contract Catalogue

The Contractor shall publish and maintain a catalogue of services delivered via this contract. The detail and format of the catalogue will be agreed between Customer and Contractor but will include, at minimum:

- Details of the goods and services provided via this contract
- Process for calling off services via the framework
- Relevant contact details

4.5.9 Exit Management

Without prejudice, the Contractor shall work with any replacement supplier of all or part of the ICT Services and with the Customer and Recipients to ensure the smooth transition of services at the end of the contract, minimising any disruption to users.

The Contractor shall prepare a documentation pack for any replacement supplier of all or part of the ICT Services that details all relevant information about the ICT Services and must clearly identify any areas when service may be lost. Any data relating to the ICT Service held by the Contractor must be returned in an agreed and appropriate format for the data type.

The Contractor shall respond to requests for information and clarification by the Customer to enable a smooth transition.

Note requirements for access and retention of documentation as per Section 4.3.2.

4.6 Procurement Services

The Customer may wish to procure ICT goods and services using its own process or with the support of the Contractor. The Contractor shall design, supply, configure and install ICT goods or services on behalf of the Customer if requested to do so.

The Customer may require the Contractor to demonstrate best value through the competition of 2 or more providers within the Contractor's supply chain. The Contractor shall provide a mechanism to compete such opportunities.

Should the Customer identify a product that is not already delivered via the Contractor's supply chain, the Contractor shall provide a mechanism for new providers to be vetted to enable such products to be procured.

The Customer will require the Contractor to provide price benchmarking on an annual basis to test for best value. A menu of items will be agreed with the Customer's Representative for the annual benchmarking.

A description of the type of ICT goods and services that may be required by the Customer follows.

- Structured cabling

- Network infrastructure
- Active network, including wireless
- Telephony
- Video conferencing
- Server infrastructure
- Server and Network monitoring
- Audio visual (AV) equipment and cabling
- End user devices
- Software deployment
- Peripherals
- Hardware as a Service
- Equipment financing/ leasing
- Refurbished Equipment (Optional)
- Administration of Parental Contribution Schemes for ICT equipment
- Provision of equipment and software for specialist subjects (i.e. Design Technology, Music)
- Assistive / adaptive devices to support Special Educational Needs
- Software (MIS, administrative, curriculum, operational, technical/management/security)
- Software as a Service
- Software design and development
- Single Sign On solutions
- ICT Consumables
- Building security systems (i.e. CCTV, access control)
- Integrated identification systems (i.e. smartcard, biometrics)
- Design and installation services for any of the supplied products
- Hosted Services, e.g. Azure, Office365, Google Apps, private cloud
- Web hosting

The Contractor must cover the breadth of these requirements through its in-house resources or via a high-quality supply chain. As and when sub-contractors are required, they must be managed directly by the Contractor and not by the Customer. The Contractor must provide the Customer with a single point of contact.

Any procurement must follow the Customer's standard procurement and approvals process and abide by EU Procurement Legislation, i.e. Public Contract Regulations 2015 and any subsequent update to these EU or other relevant UK regulations.

The process for requesting proposals and placing orders will be agreed between Contractor and Customer. Expectations for response and resolution of these requests are as per the KPIs defined in subsequent sections.

4.6.1 End-User Devices (Optional)

The Contractor must provide a number of desktop computers to a single Recipient as an option based on the specification set out below. The requirement is inclusive of supply and delivery only. The solution will be provided based upon outright purchase of 50 devices and a 3-year operating lease for the remaining 100 devices.

- 100x Desktop computers
    - No monitor required

- Ultra slim desktop chassis which includes a bracket for mounting to a VESA monitor
- 6th generation i5 processor
- 8Gb RAM minimum
- 256Gb SSD minimum
- Gigabit Ethernet Port
- 3 year next business day onsite warranty

4.6.2 Active Network (Optional)

The Contractor shall provide a scalable active network infrastructure that provides reliable connectivity.

The Contractor shall provide an enterprise-level LAN infrastructure which:

- Maximises the bandwidth between servers and the core as well as between the core and all edge devices.
- As a minimum, the bandwidth between the core switch/s and servers must support the maximum bandwidth of the server/s network interfaces.
- As a minimum, the following bandwidth shall be provided between the core switch/s and edge switch stack/s via a minimum of 2 x bonded (Active/Active) links per stack.

Number of edge switches* in a stack	Bandwidth back to the core
1 to 4	20GB
5 to 6	30GB
7 to 8	40GB
9 to 10	50GB
* Assuming a maximum 48 ports per switch	

- Maximises the bandwidth between switches within each stack. Edge switches shall be stacked using specific and dedicated stacking port/s to enable:
  - high speed communication (Minimum of 40GB per stacking module) between each switch in the stack as a part of a dedicated resilient backplane;
  - A single IP address for each stack so that the stack can be managed as a single entity.
  - Provides a minimum of one gigabit connectivity to the user device deployed to the desktop and the required bandwidth to dependant infrastructure e.g. Wi-Fi APs;
  - Can be configured and managed to support network security and quality of service; this must not impact on the network's deployment and must be aligned with the Academy environment
  - Is scalable to accommodate future developments and flexibility of deployment as well as accommodating legacy equipment as required. Contractors shall state how emerging standards might be integrated into the network; it must have a 10% surplus Power over Ethernet (PoE) to enable the deployment of additional devices in each stack;
  - Can accommodate at least one additional module per chassis (where a chassis is provided) or can otherwise be upgraded when additional capacity is required in the future;

- Has a manufacturer warranty and support arrangement (telephone, email and web), including access to software enhancements and firmware updates, providing 5 years of cover as a minimum;
- includes an onsite, manufacturer approved, system administrator training package.;
- Is Energy Efficient Ethernet compliant to a minimum of 802.3az standard;
- Has central management tools that can be used to configure the switching (core and edge), monitor performance and provide alerts in the event of a failure;
- Can support the elements of the proposed solution that require PoE, in compliance with the IEEE 802.3af/at (as required) standard, including but not limited to; wireless access points, CCTV, Access Control systems, automated registration points and VoIP equipment;
- Has a minimum of 25% PoE provision, stating how the power output is calculated and how 25% is achieved;
- Has sufficient active ports to support connectivity for 100% of terminated data points across the site including sufficient PoE for devices that require it with headroom for expansion (see expected data point number at start of this section);
- Has a core switch design that is resilient against the failure of any single component, including but not limited to redundant power supply; and
- Is suitable for integration into a wider technical solution or support arrangement, if necessary, for example an estate wide solution.

4.6.3 Wireless Solution (Optional)

Contractors shall provide an enterprise level wireless solution which will support a high number of student and staff user devices by:

- Maximising the bandwidth between the AP and the switch. Contractors shall provide a rationale for the number of data ports on the AP and the bandwidth between the AP and switch;
- Maximises the bandwidth between the AP and user devices by providing high performance AP. Contractors shall provide a rationale for the number of aerials and or spatial streams;
- Maximising AP number to ensure high backhaul bandwidth to each space, in line with the planned occupation level, to support simultaneous use without degradation in performance. Contractors shall provide a rationale for the number of Wireless Access Points (WAPs) proposed and demonstrate how this maximises the available bandwidth;
- Providing blanket coverage throughout the Academy building which ensures connectivity is maintained at a high level whilst users roam around the building;
- Providing dual band connectivity;
- Uses the fastest ratified standard at the time of installation and be backwards compatible with previous standards;
- Can be configured and managed to support network security and Quality of Service (QoS). Contractors should demonstrate how the initial configuration meets the Academy's specific requirements.
- Has a manufacturer warranty and support arrangement (telephone, email and web), including access to software and firmware updates, providing 5 years of cover as a minimum;

- Provides guest access and automated authentication for authorised users; setting out proposed initial configuration and associated capabilities specifically referring to authentication, accounting, filtering, access to content and printing;
- Where required, provides some internal WAPs to which suitable external antenna can be attached and routed to the exterior of the main building and install such antenna, should the Academy decide to purchase antenna and associated cables;
- Can actively manage and load balance user connectivity;
- Is scalable at the central controller and can accommodate future higher bandwidth requirements and/or the implementation of a resilient dual controller system; including reference to both licensing and hardware/software capacity;
- Minimises the impact of interference from adjacent networks; and
- Is suitable for integration into a wider existing technical solution or support arrangement if necessary, for example an estate wide solution.

4.6.4 Server Platform (Optional)

Contractors shall provide a server platform or equivalent that delivers a scalable, reliable and sustainable infrastructure that supports the network services described below.

Domain Controller
Contractors shall provide domain controllers that meet the needs of the Academy.

Uninterruptable Power Supply (UPS)
The Academy requires an uninterruptable power supply (UPS) which allows services to gracefully shutdown during a period of power loss. Contractors shall provide:

- Suitable UPS and relevant software to enable a graceful shutdown with notification for all servers, rated for a minimum 30 minutes and capable of providing transient over voltage protection.
- Suitable UPS for core network switches and local wireless controllers, rated for a minimum 30 minutes and capable of providing transient over voltage protection.
- Suitable UPS to enable basic environmental monitoring and remote management.

Backup
The Academy requires its data to be automatically backed up on a regular basis, to a solution which supports onsite and off-site storage and adheres to the safe and secure storage of personal and/or sensitive data line with the Data Protection Act (or subsequent data protection legislation). The following conditions must be met within the solution:

- All back-up data stored both onsite or offsite ‘at rest’ shall adhere to ISO 27001 standards for security and encryption and the DPA.
- Where data is to be transmitted over the internet (between Academy and backup provider, and between backup provider physical storage locations), use a secure transport protocol (such as SSL V3 / TLS 1.2 or better) to ensure data cannot be intercepted in transit.
- All levels of data restoration (files, whole user data, servers, entire system) in the event of complete failure or disaster.
- Current user data automatically backed up on a regular basis and historical data archived on a regular basis (regularity to be agreed at FC).
- User permissions allowing restoration of recently deleted files without the need for technical staff assistance.

- Encrypted Off-site backup that is recoverable in the event of on-site failure or disaster, with appropriate encryption key management.
- Data is backed up each night.

Directory Services
The Contractor shall provide a central directory of users and devices.

The Contractor must integrate the Management Information System (MIS). The solution must allow for all MIS software and data to be migrated to the new servers.

Storage
The Contractor shall provide a suitable scalable, reliable and sustainable storage solution. This can be on premise or cloud hosted. Storage quotas should be appropriate for the user and be easily adjustable by authorised administrators.

The Academy has Microsoft 365 accounts including One Drive. The storage solution should differentiate between the following types:

- Local storage quota allocated to users, for example teachers, administrative staff, pupils
- Local storage quota allocated to services
- Cloud storage quota allocated to users/services
- Academy specific detail and additional requirements

Collaboration and Communication Services
The Academy is looking to create an integrated environment, with the MIS as the primary database. Contractors should provide integration between the core user/device database (Active Directory or equivalent) the MIS and the online system for communication and collaboration.

Migration of Academy Data
The Contractor shall provide a solution that enables easy migration of both Directory Services and stored data from the current solution to the new systems.

Remote Desktop Services
The Academy requires designated users to have access to a remote desktop, i.e. RDS, VDI or VPN. Remote access facilities should include administrative systems, including MIS and Financial Management System.
The Academy requires these services to be accessible to admin/teaching and some support staff.

Cloud Based Services
For information, the Academy requires a mixed economy of local server client and cloud based systems. They would like Microsoft 365 accounts throughout the sites. Contractors should take account of the desire to maximise the use of cloud based software solutions.

Biometric/Card System
For information, the Academy currently uses a card based solution integrating MIS, Cunningham's Catering and Bio Store. These systems integrate to provide Academy services including access control, library system, cashless catering, including Parent Pay.

Software Deployment for learning, teaching and administration
For information, the Academy has a range of software titles that are used for administration and teaching and learning.

The Academy's have a mix of devices of varying age and specification. Where funding allows, the Academy will look to rationalise and refresh end user devices. In the future, it will be looking to make an investment in tablet devices.

For this tender assume the Trust needs to purchase:

- 100 Windows devices, including workstations, laptops and netbooks of varying age and specification. The Academy is current running the Windows 7 operating system.
- 50 Apple iPad minis

Contractors should take account of the possible requirement to provide a solution and approach for software deployment and device imaging.

This Section sets out the Service Transfer activities that the Contractor is required to provide where the Recipient instructs a form of managed service. This may include transfer from a service delivered: by an incumbent managed service provider, by a team of staff employed by the Recipient, or by a combined local and out-sourced team.

5.1 Service Transfer Requirements

The Contractor shall do all such things necessary, in accordance with the Implementation Plan to transition from existing state to the delivery of the services and to comply with the Service Levels and KPIs.

The Contractor shall be responsible for service transfer and for implementing any changes to the services with:

- Minimum disruption to staff, students, and business processes during the Service Transfer
- No loss of data during the implementation/migration

The Contractor shall facilitate effective communications and the existing service providers during the Implementation Services.

The Contractor shall appoint experienced Project Managers to be responsible for oversight of the service transfer. The Project Managers shall not be changed during the service transfer period without the prior agreement of the Customer. The Project Managers shall agree a reporting format and frequency of meetings to take place with the Recipient and Trust leads throughout the service transfer period.

The Contractor shall be responsible for demonstrating to the satisfaction of the Customer that the service transfer satisfies the requirements identified in this document before the Customer accepts them into use. The Contractor shall agree a Test and Acceptance Strategy with the Customer. The Contractor shall conduct all testing. The Customer may choose to witness any or all testing at the Customer's discretion.

5.2 Planned Commencement Dates

Academy	End Date of Existing Contract
Great Witchingham	31/12/17
Hockering	31/12/17
St Peters Easton	31/12/17
Narborough	31/12/17
Sporle	31/12/17
Castle Acre	31/12/17
Bishops	31/12/17
Weasenham	31/12/17

Where a Recipient takes up a form of managed service, the following KPIs and Service Levels should be adhered to.

6.1 Tiered Service

Due to the range of Recipients within the Trust, there is a requirement to establish a managed service provision based upon 2 tiers. Tier 2 will enable Recipients with a very low budget (i.e. small primary school) to procure a service that meets their basic operational needs. Tier 2 has been based on the requirements of two Initial Recipients that are small primary schools.

Those with a requirement for a higher quality service may purchase a Tier 1 or Tier 2 service, and add supplementary staffing or extended hours to enhance their service.

6.2 KPIs

The following table details the high-level service catalogue with expected availability during core hours. These requirements exclude planned maintenance/down-time.

Availability KPIs only apply to services delivered directly by the Contractor. Where a service is supported by a third party, availability KPIs pass over to the third party, as per their direct contract with the Customer.

Tier 1 Services	
Services	**KPI**
MIS	99.9% Availability per month in Core Hours
Finance	99.9% Availability per month in Core Hours
File & Print	99.9% Availability per month in Core Hours
Server Management	99.9% Availability per month in Core Hours
Internet Access	99.9% Availability per month in Core Hours
Email	99.9% Availability per month in Core Hours
Network Management	99.9% Availability per month in Core Hours
Telephone Management	99.9% Availability per month in Core Hours
Remote Access	99.0% Availability per month in Extended Hours
Overall Performance	
Customer Satisfaction	User survey performed every 6 months demonstrate increasing level of user satisfaction

Tier 2 Services	
Services	**KPI**

MIS	99.9% Availability per month in Core Hours
Finance	90% Availability per month in Core Hours
File & Print	90% Availability per month in Core Hours
Server Management	90% Availability per month in Core Hours
Internet Access	90% Availability per month in Core Hours
Email	90% Availability per month in Core Hours
Network Management	90% Availability per month in Core Hours
Telephone Management	90% Availability per month in Core Hours
Remote Access	90% Availability per month in Extended Hours
Overall Performance	
Customer Satisfaction	User survey performed every 12 months demonstrate increasing level of user satisfaction

Availability of key service elements will be measured based on the following service availability calculation:

$$\% \text{ Availability} = \frac{(\text{User service Hours} - \text{Downtime}) * 100}{\text{User Hours}}$$

Availability will be calculated for the service element during the standard hours based on the declared number of users of each service element.

6.3 Customer Satisfaction

The Customer wishes to manage its partnership with the Contractor in a manner that motivates the provider to achieve a high level of customer satisfaction. To monitor this the contractor will be required is to carry out a User Survey to test the level of user satisfaction. The Customer wishes to see that the results from the survey show an increasing level of user satisfaction. Therefore 5% of the contract value will be retained and paid on an annual improvement to the user satisfaction.

The Contractor shall conduct the customer satisfaction User Survey 3 months following the inception of the service to establish a baseline and once annually thereafter for Tier 1 Recipients and twice annually thereafter for Tier 2 Recipients. This will survey a minimum of 20% of Recipient staff who have used the ICT Service Desk during this period. The content and objectives measured by the survey will be agreed between the Contractor and Recipient. Examples of the areas the survey should measure include:

- The manner of the Service Desk staff
- The speed of resolution of problems
- The knowledge of the Service Desk staff
- Any use made of remote Service Desk tools

6.4 Incident Management

All Failures or potential Failures shall be allocated a priority status agreed between the Customer and the ICT Contractor based on impact and urgency.

Impact	
High	A Key Service has failed or is degraded affecting 20 or more users or A service is at risk owing to a threat or potential event e.g. virus alert, server failure or Significant risk may result from the incident, e.g. loss of revenue, reputation or security
Medium	A Key Service has failed or is degraded affecting a single user or A non-key service has failed or is degraded impacting multiple locations or users or A user's desktop has failed
Low	A non-key service has failed or is degraded affecting a single user

Urgency	
High	Critical deadlines are at risk and no workaround is available to the Recipient
Medium	No immediate deadline and no workaround is available to the Recipient
Low	No immediate deadline or a workaround is readily available to the Recipient

Priority is allocated based on the Impact and Urgency assessment as follows:

	Urgency		
Impact	High	Medium	Low
High	P1	P2	P3
Medium	P2	P3	P4
Low	P3	P4	P4

The following table details the response and resolution times according to service allocated priority during core hours. These requirements exclude planned maintenance/down-time.

Priority	**Tier 1 Service**	**Target Response Time**	**Target Resolution Time**
0	**Rapid Response** • Technical issues with a staff computer, projector/IWB and/or audio systems which prevents the teaching of a lesson in progress. • Changes to web content filtering in response to safeguarding issue	5 mins	15 mins
1	**Major loss of service** • Primary internet circuit • Major server and data storage component (i.e. domain controllers, SAN) • Major network component (i.e. switches, wireless controller) • Virus/Malware outbreak on the network • Any Priority 2 failure during the notice period of an Ofsted inspection or during the inspection	1 hour	4 hours

	• ICT equipment or critical software where a workaround cannot be found		
2	**Partial loss of service** • Component of the resilient infrastructure which is affecting system performance (i.e. an entire ICT suite, an entire laptop trolley) • Backup job failure	4 hours	1 day
3	**Minor loss of service** • Equipment failure where there is no alternative available • Non-safeguarding related change to web content filtering • Backup restores for client files	1 day	5 days
4	**No loss of service** • Non-service affecting issue which has an immediate and obvious workaround	5 days	20 days

Priority	Tier 2 Service	Target Response Time	Target Resolution Time
1	**Major loss of service** • Technical issues with a staff computer, projector/IWB and/or audio systems which prevents the teaching of a lesson in progress. • Changes to web content filtering in response to safeguarding issue • Primary internet circuit • Major server and data storage component (i.e. domain controllers, SAN) • Major network component (i.e. switches, wireless controller) • Virus/Malware outbreak on the network • Any Priority 2 failure during the notice period of an Ofsted inspection or during the inspection • ICT equipment or critical software where a workaround cannot be found	4 hours	1 day
2	**Partial loss of service** • Component of the resilient infrastructure which is affecting system performance (i.e. an entire ICT suite, an entire laptop trolley) • Equipment failure on a staff computer. • Backup job failure	1 day	7 days
3	**Minor loss of service** • Equipment failure where there is no alternative available • Non-safeguarding related change to web content filtering • Backup restores for client files	7 days	21 days
4	**No loss of service** • Non-service affecting issue which has an immediate and obvious workaround	5 days	As agreed

6.5 Service Requests in a Managed Service

The following table details the response and resolution times for service requests during core hours.

	Tier 1 Service	Target Response Time	Target Resolution Time
SR1	**Simple Change** (changes requested via the Service Desk which have a low impact on the existing ICT environment i.e. password reset, revised permissions)	1 hour	4 hours
SR2	**Standard Change** (changes which will have an impact on the existing ICT environment i.e. profile modification, data storage or mailbox settings, leaver, data restore requests)	4 hours	1 day
SR3	**Planned Project Change** (changes which are expected as part of the annual cycle that are time-sensitive enough to warrant management of the change as a project, i.e. annual transition, new starters, MIS upgrades prior to census returns)	Included in the Quarterly update of the Programme of Planned Projects, see Section 4.4.1	As per the agreed delivery date in the Programme of Planned Projects
SR4	**New Project Change** (changes which are large or complex enough to warrant management of the change as a project i.e. additions, new functionality or installation of new software components, hardware requests)	2 days (acknowledge request) + 12 days (proposal)	As agreed within proposal

	Tier 2 Service	Target Response Time	Target Resolution Time
SR1	**Simple Change** (changes requested via the Service Desk which have a low impact on the existing ICT environment i.e. password reset, revised permissions)	1 day	7 days
SR2	**Standard Change** (changes which will have an impact on the existing ICT environment i.e. profile modification, data storage or mailbox settings, leaver, data restore requests)	7 days	14 days
SR3	**Planned Project Change** (changes which are expected as part of the annual cycle that are time-sensitive enough to warrant management of the change as a project, i.e. annual transition, new starters, MIS upgrades prior to census returns)	Included in the Quarterly update of the Programme of Planned Projects, see Section 4.4.1	As per the agreed delivery date in the Programme of Planned Projects

SR4	**New Project Change** (changes which are large or complex enough to warrant management of the change as a project i.e. additions, new functionality or installation of new software components, hardware requests)	2 days (acknowledge request) + 12 days (proposal)	As agreed within proposal

In the case of service requests, Target Response Time refers to the time in which the Contractor responds to the request. For an SR1 this may simply be an acknowledgement of the request via Service Desk. For SR4 this is provision of a proposal for delivery of the change. Target Resolution Time refers to the time in which the Contractor implements the change.

SR3 Planned Project Changes will be known to both Customer and Contractor well in advance of the date in which they are instructed. As described in the Service Specification, the proactive preparation for these known events should mitigate the risk that they are unable to be delivered to the agreed service levels.

SR4 New Project Changes require agreement between the Customer and Contractor on a Resolution Time (achievement of project sign off) that reflects the scope and complexity of the project (i.e. based on delivery to time, to budget and to agreed quality indicators such as user acceptance tests), agreed on a project by project basis.

6.6 Procurement Requests not in a Managed Service

The following table details the expected response, proposal and delivery times for procurement requests by Academies that are not yet Recipients of a managed service under this contract. The approach sets expectations for a proactive sales function by the Contractor, enabling Academies to validate affordability and to place orders for new ICT goods and services via this contract in a timely manner.

	Target Response Time	Target Proposal Time	Target Delivery Time
Simple Procurement (orders requiring a low level of clarification or due diligence e.g. requests for new equipment)	1 day (acknowledge request)	3 days (proposal/ quote provided)	As agreed within proposal
Complex Procurement (changes which are large or complex enough to warrant management of the change as a project, e.g. new functionality or installation of new software components)	2 days (acknowledge request)	12 days (proposal/ quote provided)	As agreed within proposal

6.7 Temporary Suspension of Service Levels (The Pause Button) in a Managed Service

The Customer may, at any point within the term, request suspension of Service Levels in order to instruct the Contractor to participate in other relevant activities (e.g. supporting the school during an emergency, participating in a staff-wide training event on safeguarding). The Customer may be willing, for example, to accept a temporary reduction in service levels to enable staff typically assigned to delivery of the BAU service to participate in new project delivery, particularly where this provides a cost savings to the project.

The Contractor is required to offer a mechanism to enable agreed, acceptable project disruptions to the service.

7.1 Appendix A – Site Background detail

Current strategic, operational and technical details for each of the Initial Recipients have been included as an attachment within the tender package.

7.2 Appendix B – Initial Recipient TUPE Details

Intentionally blank