NEN TECHNICAL STANDARDS FOR MULTI-ACADEMY TRUSTS

NOVEMBER 2022

CONTENTS

CONTENTS COMPILED WITH THE ASSISTANCE OF MOXTON EDUCATION

Executive Summary

This document focusses on the technical aspects of implementing ICT across a Multi-Academy Trust (MAT). This brief Executive summary is designed for school leaders to introduce the concept of what, at a high level, is required to take place. The document then goes on to the technical detail, referencing the DfE standards documents where they exist and providing additional detail when they do not so that a holistic solution is referenced.

A design for ICT in Multi Academy Trusts

Preamble

This paper is to supplement the guidance published by DfE on meeting digital and technology standards in schools and colleges found at: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges

In groups of schools such as Multi-Academy Trusts it is not uncommon to find considerable variation between the solutions in the different institutions. These 'IT Islands' can represent a challenge to Trust Leadership, representing a significant risk in respect of security, manageability, cost of refresh, reliability and compliance issues. That said, overcoming the challenge is not about 'standardisation' *per se*, but on an acknowledgement that whilst school differences are key and a degree of autonomy desirable, the concept of 'harmonisation' across the group of schools should underpin the approach to the solutions adopted. This means adopting a ***common core***, particularly in respect of the technologies that are 'invisible' to users, and a ***flexible edge*** in respect of the in-school technology solutions.

Delivering the common core/flexible edge: The four-layer model:

Technical solutions can be viewed as comprising of four layers:

1. External technologies carrying traffic from/to the wall of the institution
2. Internal technologies that carry traffic around each institution's estate
3. The hardware systems that users put their hands on
4. The software applications in use

Layer One: The external technologies carrying traffic from/to the wall

The Broadband network should be harmonised across the group of schools whenever expiry of current contracts allows, even if this is done incrementally as the '***common core***' principle applies to this layer. DfE guidance on broadband is found at:

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/broadband-internet-standards-for-schools-and-colleges

Simply changing Broadband provision may not be the whole solution, however, as there are many elements inside the school which may affect the performance of the internet service. These are the 'dependencies' described in the DfE guidance and exist within the technologies found in Layer Two.

Layer Two: The Internal Technologies that carry traffic around each institution's estate

The Local Area Networks in each school also need to be fit for purpose with internal network cabling (sometimes called the passive network infrastructure) and internal network equipment (sometimes called the active network infrastructure) such as switches, routers and wireless access points (WAPs) being key to performance.

The passive network infrastructure

This element is covered by the DfE guidance:

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/network-cabling-standards-for-schools-and-colleges

The position in respect of the passive network is complex. Whilst faulty or low specification cabling will have a negative impact on the quality of network performance as it plays a critical role in the speed of data transfer, it may not be possible just to rip it out and start again as this can be disruptive and expensive. Cabling buried in walls or carried in ducts above ceilings may be an issue, as may the ducts themselves if they cannot support modern cabling.

The active network infrastructure

This element is also covered by the DfE guidance:

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/switch-standards-for-schools-and-colleges

The ***common core*** principle applies in this layer, too, so it is sensible to harmonise this provision to reduce support and maintenance costs, energy consumption and to make systems as interoperable as possible. Upgrading the active components whenever current equipment is deemed to be underperforming or out of support is the best approach, but if it is no longer possible to upgrade an active component it should be replaced as and when appropriate.

Layer Three: The hardware systems that users put their hands on

At present DfE guidance does not extend to this level, under which the vast majority of an institution's hardware estate is found. It is here that the '***Flexible Edge***' concept comes into play. This layer includes classroom toolkits and end-user devices, e.g.:

- IWBs/Display/Visualisers
- Desktop PCs, Laptops, Chromebooks, Tablets
- Peripherals like cameras/video cameras
- Robotic kits
- Specialist music devices
- Multi-Function Devices (MFDs) / printers, scanners, etc.
- Cashless catering equipment
- Access control equipment … and much more

Whilst there is no suggestion these be standardised - as the needs of different settings should dictate the chosen solution - any degree of commonality, even if there are several different 'sets' of equipment procured across a Trust, will make support easier and offer greater economy of scale in purchasing.

In making choices several considerations apply when determining a layer three asset's fitness for purpose:

- Affordability
- Usability
- Reliability/robustness
- Warranty period
- End of life disposal arrangements
- Longevity
- Energy consumption
- Carbon footprint
- Security
- Upgradeability

Layer Four: The Software - such as productivity & curriculum software, the MIS & other back office administrative apps

Again, at present DfE guidance does not extend to this level, and whilst the '***Flexible Edge***' concept is still key in respect of curriculum applications, where possible 'back-office' and key administration applications should be harmonised if they are used Trust-wide. In particular, having a common set of systems like the MIS, Finance/Payroll, HR, Safeguarding, Visitor Management and so on has real benefits. Duplication of functionality should also be avoided, with the purchase of specialist applications for the likes of Behaviour & Rewards or Assessment being carefully considered against using the native functionality in the MIS. A similar argument applies to Trust-wide analytics, reporting and dashboarding – where possible use the MIS tools or change to an MIS that has them! Handled properly, a rationalisation of the existing provision and eliminating the need for additional purchases can simplify day-to-day operations and save a considerable amount of money.

Fundamental Technical Principles

The fundamental principle behind this document is that schools should take advantage of public cloud services where it is commercially advantageous to do so. At the time of writing this document, this typically means the use of either Google Workspace for Education or Microsoft 365 both of which offer significant cloud-based tools, elements of which are free of charge for education establishments. It is expected that these services will form the basis of the school's ICT systems and it's likely that some additional bolt-on services or bundles will be required for either system.

In the MAT context, it is expected that any cloud service would be provisioned as a single tenancy across the Trust rather than individual systems within each of the schools. This will enable the Trust and schools to collaborate seamlessly within the relevant tool, not least as there will be a single directory of users across the Trust solution. This will allow the Trust to pool and share knowledge across the schools, including (but not limited to):

- Trust-wide policies and procedures
- Curriculum strategy
- SEN information
- Lesson plans

Consolidating schools to a single cloud service may be challenging; schools joining the Trust may not be using the same cloud solution that the Trust has chosen. This typically relates to the platform chosen for use in the curriculum rather than for staff – for example a school may have years of information in Google Classroom and may be resistant to migrating to a Microsoft 365 platform. In this situation the Trust can consider the deployment of multiple cloud platforms as long as there is a clear strategy around the availability/location of key information. Many Trusts, for example, have a Microsoft 365 platform for Trust/School staff collaboration and use Google for interaction in the curriculum. In this scenario, there is still sense in consolidating to single Trust-wide tenancies of all cloud systems rather than maintaining individual school tenancies.

Local Services

The following services will typically operate from equipment based on-site in the school (i.e., not available over the internet connection/cloud services). The equipment hosting these services will vary by ICT supplier:

- DHCP services
- File shares for:
    - Legacy data (where absolutely essential and for data that the school does not want to be located in the cloud)
    - Academy specific purchased content (where no cloud option is available for that content)
- Print queues and any legacy print management systems
- Backup of cloud services data (unless a second cloud backup service is in use)
- Any other school specific system which cannot be operated from the cloud services (examples may include older MIS/finance system products, older telephony services, door access control systems, cashless catering systems, CCTV systems or BMS [building management systems])

Note: schools should be planning to reduce the need for on-premise systems which may require a server. Therefore, consideration should be given to any future purchase of equipment which may have a dependency on local servers (e.g., CCTV, door access control, cashless catering, admin/curriculum applications/content). In many cases cloud versions are available or are in development with suppliers.

Cloud Services

The following services will typically be located in the Cloud/3rd Party provider:

- Education collaboration services through Google or/and Microsoft 365 (Google Classroom or SharePoint/Teams)
- Email through Google or/and Microsoft 365 (Gmail or Exchange Online)
- Google or/and Microsoft 365 for user data storage (Google Drive or OneDrive)
- Device Management, including the management of operating system updates (Google for Chromebooks, Microsoft Intune for Windows/Apple devices or 3rd party for Apple, if Intune is not sufficient)
- School MIS / Finance systems (where possible)
- DNS services (using a public DNS supplier)
- Telephone services (if not an older, on-site system)
- Network and wireless management systems (subject to a subscription – note this subscription should not be a mandatory requirement for the functionality of the network/wireless systems, just for management)
- Multi-factor authentication
- Backup of Cloud data (unless an on-site backup device is used)
- HR/Payroll services

Notes:

1. Some Trusts may wish to host a number of the above functions on their own, central infrastructure operating from a Trust location. This needs careful consideration in terms of backup and data security. Such a system would typically have a centralised Active Directory across all schools with each school operating as a subset within the management tools. This provides a high degree of control and flexibility where there is a dedicated IT Support Team within the Trust. However, there are risks around the potential wide-spread exposure if any of the schools were subject to a cyber-attack. In a single Active Directory system each school is generally visible from the others, this means that a successful cyber-attack at one of the schools could result in a Trust-wide data breach as hackers may be able to easily traverse the links between schools.
2. The section above discusses the use of Google or/and Microsoft cloud tools, whilst there would be significant benefits to standardising on one platform in terms of the user experience and there being a single system for all users to access, it may be that Trusts would benefit from the use of both systems in parallel; for example it may be that Staff use the Microsoft cloud platform for collaboration across the schools and Trust but that Google is used for teaching and learning. This would allow Trusts to leverage the best of both systems, however, there would need to be clear 'sign-posts' to ensure that staff users (who would generally be accessing both systems) have a clear understanding as to which system is used for what purpose.

Connectivity

Trust schools should have a broadband connection capable of supporting the use of the cloud systems. The connection should be based on the following specifications:

- Full fibre-optic (sometimes described as leased lines or fibre to the premises [FTTP] – older, copper connections do not meet the standard and should be avoided)
- Primaries – Equally fast in both directions (synchronous) upstream and downstream. If this is not possible, primary schools should have a minimum 100Mbps download speed and a minimum of 30Mbps upload speed (schools larger than 500 pupils should consider 200Mbps download/100Mbps upload connections)
- Secondaries – 1Gbps speed and equally fast in both directions (synchronous) upstream and downstream (schools larger than 1,200 pupils should consider 2Gbps synchronous connections)
- Uncontended – i.e., not shared with others
- Easily and affordably upgradeable
- Redundant – i.e., a second or back-up line should be included, and this back-up line should ideally be diversely routed and terminated on parallel equipment in the school so as not to be hostage to a single event like accidental /

deliberate vandalism and/or a Network Operating Centre failure. This backup line may operate at a reduced speed in comparison to the main connection

- Safe and secure – with the school protected from:
    - Hacking, Penetration, Data Theft, Ransomware attacks, etc.
    - Deliberate Denial of Service attacks

  This means connections should be properly protected by firewall devices. This firewall should be managed by the broadband provider on behalf of the school, subject to a documented Change Control process

Internet Filtering

All access to the internet should be filtered through an educationally relevant internet filtering system such that pupil access is filtered and monitored in accordance with the 'Keeping Children Safe in Education' document, paragraphs 140 – 147 (2022 document). This should be achieved using a product which meets the requirements and should ensure granular control of internet access for all users. Schools can consult the UK Safer Internet Centre to choose an appropriate product/supplier (https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses)

An appropriate system will recognise the individual user using each device and filter internet access according to the profile of the user (i.e., a teacher would expect to experience a different level of filtering to a pupil). For secondary schools, such a system can be used to provide additional granularity based on the maturity of the pupils (e.g., Sixth Form users may be configured with a different level of filtering to earlier years in the same school). All pupil internet browsing should be recorded such that an individual's access can be tracked if required.

For multi-academy trusts, a single cross-trust platform should be considered which allows central Trust staff to monitor internet usage across all schools through the use of a single management system. This will also allow for the centralisation of alerting to a central safeguarding team, if appropriate.

Where practical the filtering system should be configured to automatically send scheduled and/or real-time alerts to the school's Designated Safeguarding Lead, highlighting any inappropriate access.

Trusts and schools should consider their off-site internet filtering requirements. This may be for school owned pupil or staff devices which are taken off-site. Modern filtering platforms frequently support on-device filtering managed through a central platform. This should be considered in conjunction with an Approved Use Policy (AUP) for both pupils and staff.

User Directory Services

Underpinning any multi-user ICT system is an underlying User Directory. This is true for on-site or cloud hosted systems. Schools and Trusts should consider the use of appropriate tools to link their MIS to the user directory such that users are automatically created in the relevant directory when the user is added to the school's MIS. The system would then email back to the school the relevant user details that have been created.

Such a system will ensure that users are created automatically against a set of pre-defined rules. The system will also be able to pull across class and timetable information, which can then feed into the relevant cloud provider's systems to setup relevant groups which can be used in remote teaching tools.

Systems such as these reduce the management overhead for schools and trusts as system users will be automatically created and deleted based on the information in the MIS. Many vendors' systems include additional functions which manage cloud platform licensing based on the MIS information, significantly reducing the management time around user management.

Multi Factor Authentication (MFA)

MFA should be used for all staff at a minimum and should protect access to all cloud services and management systems (where supported by the provider). MFA is typically achieved using a mobile phone device with a relevant provider's authentication app (e.g., Google or Microsoft Authenticator). However, where users strongly resist the use of a mobile phone device, dedicated hardware-based tokens can be used, which are purchased for each individual needing a token.

Cyber Essentials

The Academy's Finance Handbook makes a recommendation that Academies and Trusts should look to complete Cyber Essentials. This is an important benchmark which can be used by Trusts to ascertain how their ICT systems are protected from potential cyber-attacks. As such Trusts should review their ICT systems holistically in order to understand any potential weaknesses/areas for improvement.

Once the Trust has completed their own assessment satisfactorily, then progressing down the formal Cyber Essentials / Cyber Essentials Plus certification should be considered. Trusts should consider this an independent audit of their systems. Any recommendations/areas of improvement MUST be acted on in order for the Trust to be comfortable in the security of their systems. Typically, Cyber Essentials audits allow a period of time for rectification work to take place within the cost of the initial certification exercise.

Cyber Essentials Plus includes an on-site audit to verify the information that the trust provides through the Cyber Essentials self-assessment and should be considered the baseline for trusts to aim for.

Servers

As discussed above, there is a strong likelihood that some schools, especially in the secondary phase, will need to retain local servers on-site. Where this is necessary, the server system should be of the following minimum specification, although your ICT Supplier may recommend a specification specific to your requirements:

Notes:

1. **As mentioned above, schools and Trusts should be looking to reduce the need for on-premise server infrastructure, indeed if the school/Trust has already fully committed to a Google or Microsoft cloud platform then there may not be any servers in place currently**
2. **ALL servers should be genuine UK stock with manufacturer backed support and warranty**
3. **Ensure that the specification of any server device allows for the operation of Police CyberAlarm in addition to any specific requirements of the school** (https://www.cyberalarm.police.uk/)
4. **It is assumed that a secondary school will require a server system comprising of a minimum of two servers, this will allow for resilience and will allow the school's support teams to carryout maintenance/updates to the system without having to shut down the whole system. Alternatively, schools could choose a single server, however, the SLT will need to schedule in a monthly maintenance window to allow the support team to carryout monthly system updates.**

Minimum Recommended Hardware Specification – Primary Schools

Small form factor server device (tower PC size or equivalent)

4 core processor

Minimum of 32GB RAM

2x 200GB SFF SATA SSD for Operating System, configured as RAID1

2x 2TB SFF SATA SDD for DATA, configured as RAID1 as a minimum

Hardware RAID controller

2 x 1Gbs RJ45 network connections

Dedicated hardware based remote management capabilities, including the ability for a support provider to remotely control the server console at a hardware level

TPM 2.0

5yr next business day warranty

Minimum Recommended Hardware Specification – Secondary Schools

Dual Server

(Where more than two servers are required, the specification below can be multiplied up as needed)

1 or 2U rack mount chassis (depending on the quantity of required hard drive slots)

2 x 10 core processor

Minimum of 64GB RAM (depending on the quantity of virtual servers running on this machine – do NOT over allocate the memory to virtual servers!). Note sufficient memory should be available in each server to allow ALL virtual servers to operate on one server in the event that the second server has failed or is in 'maintenance mode'

Minimum of 2 x 480GB SFF SSD for Operating System in RAID1 configuration

Hardware RAID controller, with battery backed cache

Minimum of 2 x 10Gbps (or higher) network interface card with appropriate connectors for the school's switches (usually SFP+)

2 x 1Gbps UTP network interface cards

Dual Power Supplies

Hardware based remote control and monitoring tools integrated into the server, any licensing should be for a period of 5yrs, if perpetual is not available

TPM 2.0

5yr on-site hardware support (next business day fix as a maximum)

Shared Storage

For the servers above to operate as a highly available cluster (where one of the hosts can fail or be taken offline for maintenance without affecting the functioning of the school's IT systems) some form of shared\replicated storage is required. This can be achieved by implementing either:

A storage area network (SAN) device – this is a dedicated device providing high-speed network-based storage. If considering this, then it should conform to the following standards:

- Minimum of 2 x 10Gbps+ connections to each host server
- Appropriate hard drives (capacity and performance [SSD or HDD]) to support the needs of the school
- Appropriate disk resilience to include two drives for parity (RAID6)
- Spare drive bays to allow for increasing the storage without needing to purchase additional server hardware

Virtual Shared Storage – vendors such as Microsoft and VMware support virtual storage solutions which share and replicate internal server storage between multiple hosts. If considering this option, then schools should ensure that the system design has been verified by the appropriate manufacturer as being suitable for the chosen solution. In addition, it should conform to the following standards:

- High speed, resilient, dedicated network connections (25Gbps+) between the host servers for data replication
- Appropriate hard drives (capacity and performance [SSD or HDD]) to support the needs of the school
- Spare drive bays to allow for increasing the storage without needing to purchase additional server hardware

Single Server

1 or 2U rack mount chassis (depending on the quantity of required hard drive slots)

2 x 10 core processor

Minimum of 64GB RAM (depending on the quantity of virtual servers running on this machine – do NOT over allocate the memory to virtual servers!)

Minimum of 2 x 480GB SFF SSD for Operating System in RAID1 configuration

Minimum of 4 x 2TB+ SFF SAS HDD for Data in RAID6 configuration (sufficient disks should be purchased to provide the required storage, noting that RAID6 will retain 2 drives for resilience – in this example, c.4TB will be useable)

Hardware RAID controller, with battery backed cache

Minimum of 2 x 10Gbps network interface card with appropriate connectors for the school's switches (usually SFP+)

2 x 1Gbps UTP network interface cards

Dual Power Supplies

Hardware based remote control and monitoring tools integrated into the server, any licensing should be for a period of 5yrs, if perpetual is not available

TPM 2.0

5yr on-site hardware support (next business day fix as a maximum)

Operating System Licensing

Note:

1. If a school/Trust has already fully committed to a Google or Microsoft cloud platform then there may be no need for an on-premise server and any associated licensing, therefore, this section only applies where a server IS required on-site

Primary Schools

It would be expected that a Primary School is unlikely to require more than two virtual servers operating on any hardware-based server. As such, the school should ensure that they have appropriate licenses to support two servers. In the case of Microsoft licensing, this would mandate a minimum of a 16 core Windows Server Standard license[1] – this allows for the server itself and two virtual servers to operate.

Your ICT supplier should be able to advise you on the correct version of Windows Server to use based on the school requirements. However, school should aim to use the latest stable release to ensure longevity of support for the server (Windows Server 2022 is the current version at the time of writing this document).

Secondary Schools

A Secondary School would be expected to have a number of virtual servers operating in the school (even if the school is making use of Cloud storage for user and shared data). As such, the school should ensure that they have appropriate licenses to support the physical and virtual servers required. In the case of Microsoft licensing, this can be achieved through two methods:

Windows Server Standard – with each Windows Server Standard license you have the right to run two virtual operating systems. Multiple Windows Server Standard licenses can be purchased to support the quantity of physical

[1] Note that Microsoft mandate a minimum of 16 processor core licenses for a Windows Server Standard license, however, if you have a server with more than 16 physical processor cores installed, then you will need to increase the number of Windows Server processor core licenses to match the number of physical processor cores. Also note that if more than two virtual servers are required, then additional licenses will be required in multiples of 16

and virtual servers required. For example, running 10 virtual servers would require 5 Windows Server Standard licenses, licensed for an appropriate number of physical server processor cores. Any Windows virtual servers added in the future will require additional licenses to be purchased.

Windows Server Datacentre – with each Windows Server Datacentre license you can run an unlimited number of virtual Windows Servers on the licensed physical server, which must be licensed for the number of processor cores as per Windows Server Standard above. For example, a school running 10 virtual servers on one physical server would only require one Windows Server Datacentre license (licensed for the number of processor cores). Any additional Windows virtual servers added on the licensed physical server would NOT require any new licenses to be purchased. Two or more physical hosts would require a Windows Server Datacentre license for each of the physical hosts (with the relevant number of processor cores licensed)

Your ICT supplier should be able to advise you on the correct version of Windows Server to use based on the school requirements. However, school should aim to use the latest stable release to ensure longevity of support for the server (Windows Server 2022 is the current version at the time of writing this document).

Virtual Server Specification

Where using virtual servers, schools should ensure that the servers are built with 'thick' provisioned storage – this prevents the storage being over-allocated which could lead to issues in the future. Virtual servers should be built to a specification which meets the requirements of the server without exceeding the available physical resources in the server, allowing sufficient resources for the server itself to operate (e.g., if the server has 32GB RAM, then no more than 28GB should be allocated across the virtual servers).

Server UPS

Any server device should be connected to an Uninterruptible Power Supply (UPS), rated to support the running of the server for at least 10 minutes, whilst allowing sufficient battery power for the server to shut down gracefully (i.e., not simply switch off). The school should consider purchasing a new UPS device in conjunction with any new server in order to ensure that they're not relying on an old system. Schools should be aware that most UPS devices are based on lead-acid batteries which degrade over time, so schools should expect to renew batteries on a regular cycle (perhaps every 3yrs or so).

System Administration Accounts

Schools and Trusts need to carefully consider what system administration accounts are in use and how they're used. Good practise would include:

- Never use a network system administration account for day-to-day activities (such as reading email, internet browsing and/or downloading files from the internet). System administrators should have a personal 'standard' user account for day-to-day activities and a separate system administration account. This reduces the risk of malware accidentally being introduced into the system
- Never share system administration accounts between users – each member of staff/3rd party contractor needing system administration privileges should have an individual named account
- Consideration should be given to disabling the default 'Administrator' accounts (only if alternative accounts have been created first). Usernames such as 'Administrator' or 'Admin' are prime targets for potential hackers trying to access the system
- Consideration should be given to enabling multi-factor authentication for system administration access to the local network (in addition to administration access to any cloud service)
- If a 3rd party needs system administration access to the system, then this should only be granted if confirmed it's absolutely necessary and any such access should be through a named account which is set to automatically expire once the 3rd party's work is complete.

System Service Accounts

Where there is an on-site system, system service accounts may be required for certain applications to function (e.g., backup). Schools should take a zero-trust approach to these service accounts and grant the minimum access necessary for the application to function. Simply giving an account 'Domain Admin' access is not good practice.

Where possible system service accounts should be configured to 'Deny Logon Locally'. This will reduce the risk of a hacker using a service account to access the school network.

Anti-Virus

Trusts should ensure that there is an appropriate anti-virus system in place. This should be configured for real-time scanning on all devices and weekly full scans of the local drives, at a convenient time when the devices are likely to be switched on (perhaps first thing in the morning, before the school day?).

The anti-virus system should include a central management tool (likely based in the cloud) which can report the status of all devices across the Trust. This system should be configured to ensure that the anti-virus definition files are no older than 12 hours from those available on the manufacturer's website.

Reporting should be configured on the anti-virus console such that the person(s) responsible for managing the system receives alerts advising of any virus infection that cannot automatically be resolved by the system itself, any such alerts should always be investigated by the Trust ICT support team.

Google ChromeOS devices are designed to be more secure than other operating systems and have built in anti-virus systems. This along with centralised management and application deployment should result in a reasonably secure environment. However, Trusts should consider deploying anti-virus software across their Chrome OS devices, especially if the trust has anti-virus licenses available.

Anti-Malware

Trusts should implement anti-malware software (some schools may have this bundled with their broadband connection). Where such a system is used, the anti-malware software should conform to the same principles as the anti-virus software above.

Operating System & Firmware Updates

Trusts must have a register of key devices/systems in place. This should clearly show the following details:

- The function of the device/system
- The manufacturer and model number of the device/system
- The date the device/system was purchased
- The expiry date of any support purchased with the device/system
- The version of installed software/firmware on the device/system (this information should be updates if system updates are applied)

Where practical, trusts should ensure that they are using devices which are capable of running a fully supported version of the relevant operating system. Appropriate manufacturer or 3rd party management systems (e.g., Windows Server Update Services) should be used to ensure that the devices are fully updated with the latest updates within 14 days of the update being made available.

Where there is no manufacturer or 3rd party management system, the trust should ensure that the person/organisation responsible for the ICT system carries out at least a quarterly check of the items on the register to validate whether there are any critical updates which need to be applied to the device/system. Any such updates should be applied as soon as possible. If the device/system is not capable of being updated then the trust should consider disposing/replacing the device or system!

Police CyberAlarm

Where supported by the schools' broadband providers and where there is an appropriate device within the school to host the service, trusts should implement the Police CyberAlarm[2] (PCA). Schools should register for this individually at https://www.cyberalarm.police.uk/. This will collect system data from the school's firewall and forward it a central repository for trend analysis (no user or confidential data is recorded).

Police CyberAlarm will need to operate on a server device located within the school and should be factored into the specification of any server above.

DHCP Services

Schools, or their ICT supplier, will need to ensure that there is a Dynamic Host Configuration Protocol (DHCP) service in place, this is typically located on a server but can also operate on a network switch or firewall device. The DHCP server will allocate unique IP addresses to the school's device, along with any other required information needed to communicate with the internet. Typical DHCP settings include:

Range of IP addresses to allocate

Network subnet mask

Default gateway (router IP address)

DNS server address

Any telephone system specific information

DNS Services

Schools or their ICT supplier will need to ensure that DHCP is providing the details of an appropriate Domain Name Services (DNS) server. This is likely to be the local server (if a server is present) or it could be your broadband provider or a public DNS server on the internet (e.g., Google's public DNS service).

Backup

Trusts need to pay careful attention to their backup strategy, it's important that school and trusts understands what data they have, where it's stored, where it's backed up to, how frequently and how long the backup is stored for?

Again, the DfE RPA mandates a structured approach to backup which should include the following key principles:

- Ensure that backups are not stored in a location which is easy for a hacker to access (i.e., don't use a constantly connected USB hard disk)
- Ensure that there is a copy of backup data in an offline storage location (ideally located in the cloud somewhere….but not the same cloud where you have your main data stored)
- Ensure that only authorised users have access to your backup data.

The nature of cloud storage is that it is not online storage to the local on-site system. Cloud has to be accessed either by a user or a specially configured piece of software, therefore, it's inherently more secure than local storage, subject to suitable password strength.

[2] Note that registering with PCA is mandatory for academies wishing to join the DfE's Risk Protection Arrangement (RPA)

Here are two scenarios around backups:

Scenario 1 – school data in the cloud

In this scenario the school has all their data stored in the cloud (either Google or Microsoft 365), whilst both providers have a rudimentary data retention policy, it's not a backup solution. The standard offerings are essentially the same as the Windows Recycle Bin – a user can recover a delete file themselves for a period of up to 90 days. For a full backup, the school/trust would either:

- Purchase a secondary cloud backup service (which would take regular backups of the live cloud data). This would act as a full backup and keep data for as long as the system is configured, up to the amount of storage purchased by the school

or

- Purchase an on-site storage device (which would stay on-site in the school), with appropriate software which would backup the cloud data and store it on the device. It's important this device is dedicated to the backup function and is not used for other purposes

Scenario 2 – School has on-site servers

In this scenario, the school has on-site servers, which need to be backed up. In this case, the school would need to purchase a backup storage device, some backup software (which includes the ability to back up to a cloud storage provider) and some cloud storage. This system would back up the school servers to the storage device but then also take an additional copy and store it in the cloud storage area.

In all cases the backup systems should be monitored to ensure that the backup is functioning correctly, and a regular testing regime should be implemented to ensure that the backups can be used to restore data. Any testing should include a full restore of a system/service rather than simply restoring individual files.

Network Switching

A Secondary School is likely to have need of a core switch, this will allow the school to separate different types of devices at the network level (VLANs) and apply different security profiles between these VLANs. Primary schools may not need a core switch as such, unless the school is a very large primary school (in which case it may be sensible to treat the school as a small secondary)

Core Switch

A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to the wider network:

* Quantity of Core Switches will depend on the number of remote hub rooms and any server devices which will connect to the core switches:

- There should be a minimum of two switches (or a chassis device with dual management modules)
- The switches should have dual power supplies
- Where multiple switches are used, the switches should stack at a minimum of 40Gbps, using dedicated stacking ports
- Must support current mix of fibre types and copper Ethernet including
  - Minimum of 24x copper UTP ports appropriate to the devices needing to connect (e.g., some devices may require 2.5, 5 or 10Gbps)
  - Support POE appropriate to the devices needing to connect
  - Appropriate number of 10Gbps+ ports for the number of hub rooms, such that each hub room is connected with a minimum of 2 x 10Gbps+ links (with at least 2 spare ports)
- Support layer 3 switching, VLANs, access control lists and spanning tree support
- Should support:
  - 512MB minimum memory
  - Minimum of 16,000 MAC addresses
  - Use non-blocking switch fabric

- Rack mountable
- Support integration into a central configuration management platform with 5yr license included
- All core switches must have the manufacturer recommended software\firmware installed
- Lifetime warranty

Access Switches

Access switches are the only switches that directly interacts with end-user devices. Because an access network switch connects the majority of devices to the network, it normally has the highest port density of all switch types:

*Quantity of Access Switches will depend on the amount of end devices in each area

- Either individual 1U switches or a chassis switch
- Where multiple switches are used, the switches should stack at a minimum of 40Gbps using dedicated stacking ports
- The switch, or stack of switches, should support 2 x 10Gbps+ network links to the main core switches
- Where high-speed Wi-Fi 6+ access points are in use, the switches should support 2.5, 5 or 10Gbps connections to maximise wireless throughput
- Rack mountable
- Support integration into a central configuration management platform
- Must support 802.11af or 802.11bt appropriate to the devices needing to connect (e.g., high-performance Wi-Fi 6+ access points will require higher power)
- Should support LLDP-Med
- Should support:
  - 512MB minimum memory
  - Minimum of 16,000 MAC addresses
  - Use non-blocking switch fabric
- All access switches must have the manufacturer recommended software\firmware installed
- Lifetime warranty

VLANs

VLANs may need to be configured to ensure separation of network traffic for guest wireless users, the switch specifications above support the use of VLANs.

Primary schools may not be large enough to justify the additional complexity of implementing VLANs

In a secondary school it is expected that the school would consider the structure of the network and apply additional VLANs to provide network separation between devices. This could either be based on device types (e.g., curriculum devices, admin devices, teacher devices, printers, etc.) and/or could be based on the physical spaces in the schools (e.g., admin block, science block, technology, etc.)

Network Patching

Trust should try to follow a patching colour scheme – this helps with the diagnosis of faults in the future (the scheme should be documented and a list showing the purpose of each colour cable kept in each network cabinet location). Keeping this consistent across a Trust will simplify the support of all schools and allow any support staff to visit any of the schools and be comfortable that they are operating to the same standard. An example is shown below:

Device	Colour
Servers	Yellow
Wired	Grey
Access Points	Red
Printers	Purple
CCTV	Black
Telephones	Green

Management

Trusts should look to deploy a cloud management system for their network equipment (switches and wireless) such that there is a single management dashboard across the Trust. This will give the Trust's support team full visibility of the network estate to ensure that the system is operating effectively. This should also allow for the remote management and configuration of the network devices, as needed.

Wireless

Surveys

Trusts should work with their ICT Supplier to carry out a survey of their schools to ensure that an appropriate number of wireless access points are purchased to provide coverage across the whole school. This may include external wireless access points if the school needs wireless coverage in certain areas outside of the school buildings (note, there is likely to be some coverage from access points within the building, but this may be limited in terms of performance and range)

Hardware Specification

Wireless access points should be a minimum of:

Wi-Fi 6 (802.11ax)

Support 2x2 MIMO as an absolute minimum

Support 2.4GHz and 5GHz

Support either an on-site controller, use of an access point as a controller or integrate with a cloud hosted controller (note, the use of a dedicated on-site controller is the least preferred option)

802.11af PoE powered

Support multiple SSIDs

Support RADIUS authentication

Support secured guest wireless access through the use of a time limited user account, managed by non-technical staff

Guest access should be separated from the main network such that access to any on-site server devices is not possible

Appropriate speed network interface as needed to support the maximum performance of the access point (i.e., 1, 2.5, 5 or 10Gbps)

Lifetime warranty

Full Apple Bonjour support across VLANs

External access points should conform to the minimum specifications above

Wireless Networks/SSIDs

Wireless networks/SSIDs should be created as appropriate for the school /Trust use, as a minimum this is expected to be:

SSID for Trust managed devices (likely to be split as staff and pupil SSIDs)

SSID for roaming Trust central users to allow central staff to move seamlessly between sites

SSID for guest users - This SSID should restrict access to internet services only and prevent access to the local servers. A guest network should be filtered to a similar level as the pupils.

Others may be required depending on the school's requirements.

Wireless Security

Where possible wireless security should be configured such that, no un-authorised access can be obtained to either the main wireless SSIDs or the Guest SSID. Schools should consider the use of named accounts for guest access.

For trust owned, managed devices consideration should be given to integrating the directory service into the wireless network such that managed devices need no additional authentication.

Access Point Mounting

An appropriate survey (either paper based or physical) should be carried out using appropriate survey tools to establish the wireless access point quantities and locations based on each school's requirements. Access points should be mounted as per manufacturer recommendations (usually ceiling mounted). Where the access point is not visible (e.g., installed in a ceiling void or behind an obstruction), then an appropriate label should be mounted adjacent to the access point location to allow easy identification.

Workstations/Laptops

All devices should be UK stock from an authorised reseller

Warranty Requirements

All new desktops and laptops should be provided with the following warranty cover:

Desktop Devices (including Apple desktops)

5 years on-site, next business day warranty

Laptop Devices (including Apple laptops)

Minimum 3 years return to base, 5-day turnaround from receipt warranty

Minimum Recommended Hardware Specification – PC / Laptop Devices

All newly purchased workstations should meet the following minimum specifications:

Note: All mobile devices should be capable of being charged via USB-C

Device Type	Vendor	CPU	RAM	SDD (GB)	GPU	Screen Size	Operating System	Wi-Fi	Warranty
Staff - All in One Desktop	Tier 1	Latest Gen Intel i5	16GB	512	Integrated	24"	Windows 11	Wi-Fi 6	5 years
Staff Laptop Touch screen	Tier 1	Latest Gen Intel i5	16GB	512	Integrated	13-14"	Windows 11	Wi-Fi 6	5 years
Staff Laptop Non-touch screen	Tier 1	Latest Gen Intel i5	16GB	512	Integrated	13-14"	Windows 11	Wi-Fi 6	5 years
Student All in One Desktop	Tier 1	Latest Gen Intel i3	8GB	256	Integrated	22"	Windows 11	Wi-Fi 6	5 years
Student Laptop Touch Screen	Tier 1	Latest Gen Intel i3	8GB	256	Integrated	11 -13"	Windows 11	Wi-Fi 6	5 years

High Specification Desktops	Tier 1	Latest Gen Intel i7	16GB	512	Dedicated	24”	Windows 11	Wi-Fi 6	5 years

Minimum Recommended Hardware Specification – ChromeOS Devices

All ChromeOS hardware should be purchased via an authorised reseller and enrolled into the Trust’s Google Workspace for Education platform. This will require the purchase of a Chrome Device Management license for each device.

Device Type	CPU	RAM	Storage (GB)	Screen Size	Connectivity	Warranty
Desktop	Dual core	8GB	128	24”	1Gbs LAN + Wi-Fi 6	5 years
Staff Laptop Non-touch screen	Dual core	8GB	128	14”	Wi-Fi 6	5 years
Staff Laptop Touch screen	Dual core	8GB	128	14”	Wi-Fi 6	5 years
Student Laptop Non-touch screen	Dual core	4GB	64	12”	Wi-Fi 6	5 years
Student Laptop Touch screen	Dual core	4GB	64	12”	Wi-Fi 6 only	5 years
Tablet	Quad core	4GB	64	11”	Wi-Fi 6 only	5 years

Minimum Recommended Hardware Specification – Apple Devices

All Apple hardware should be purchased via an Authorised reseller and enrolled into the Trust’s Mobile Device Management system. Apple desktop devices should include a WIRED keyboard and mouse rather than wireless

Device Type	CPU	RAM	Storage (GB)	GPU	Screen Size	Operating System	Connectivity	Warranty
iMac	M1	8GB	256	Integrated	24”	Latest Mac OS	1Gbs LAN + Wi-Fi 6	5 years
Mac Mini	M1	8GB	256	Integrated	22” monitor required	Latest Mac OS	1Gbs LAN + Wi-Fi 6	5 years
MacBook Air	M1	8GB	256	Integrated	13.3”	Latest Mac OS	Wi-Fi 6	5 years
MacBook Pro	M2	16GB	512	Integrated	13”	Latest Mac OS	Wi-Fi 6	5 years
iPad Pro (power users)	M1	8GB	126	Integrated	11” or 12.9”	Latest IOS	Wi-Fi 6 only	5 years
iPad Air	M1	8GB	64	Integrated	10.9”	Latest IOS	Wi-Fi 6 only	5 years
iPad Mini	A15	4GB	64	Integrated	8.3”	Latest IOS	Wi-Fi 6 only	5 years

iPads should be supplied with full body protection cases, including screen covers

Apple TV

HD –

32GB Storage

Wall Mount / Lock

4K –

32GB Storage

Wall Mount / Lock

Laptop Docking Stations

Laptop docking stations should meet the following specification:

USB-C connection which supports charging (a USB A to C converter can be used where legacy laptops do not have a USB-C connection)

1Gbs Ethernet port

Minimum 1 x HDMI 2.0 port

Minimum 4 x USB 2.0 / 3.0 ports

Support USB-C charging up to 100W

Universal docking station so will work with different vendors/brands

Hardware Specification – Laptop & Tablet Charging Units

Laptop/Tablet Units

High quality steel construction

Secure locks

Support charging of all devices through a single power cable

No interference to wireless network coverage for devices whilst in the unit

Be available in different device capacities

Support large rotating castors for easy mobility

Support laptops with up to 16” screens

Easy access for cable management

Active ventilation should be included

Device Operating System

The device should ship with an appropriate Operating System pre-installed based on the device. For Microsoft Windows devices, the school should engage with their ICT Supplier to confirm the most cost-effective option. Schools frequently have a Microsoft Volume License agreement which includes a license to upgrade to Windows Education version.

Laptop & Desktop Device Encryption

Schools must ensure that any device that is taken off-site has appropriate disk encryption software configured. For Windows devices, this is Bitlocker. This will provide an additional level of protection if a device is stolen or lost – the hard drive cannot be installed in an alternative device and data extracted from it.

Remote Access

This document is written on the assumption that the Trust will operate with a cloud storage provider(s); as such, remote access into any of the schools should not be required. Trusts and Schools must be very careful to ensure that they are not opening possible 'back doors' into the system by allowing remote access. This includes the use of remote support tools which are often used by 3rd parties to support their systems – these should not be left running but should be initiated by somebody in the school in the event of a problem and closed/disabled when the remote support is completed.

Many secondary schools will operate external remote access services, such as Microsoft Remote Desktop Services. As above, Trusts must be aware that any such system is a possible attack point for hackers, therefore, the following should be considered if such a service is in place:

- Never publish links to such services on any Trust or school website
- Always ensure that the system is using the latest possible software/firmware (if this is not possible then trusts should consider retiring/replacing the service)
- Consider enforcing two factor authentication
- Consider regular vulnerability/penetration testing to validate the security of the network (and ensure any issues identified are investigated and addressed)

Printing

Trust should consider reducing the number of expensive desktop printers and move to a centralised print model using large multi-function devices (MFDs) / photocopiers across their schools. This will massively reduce the Trust's printing costs and make the system easier to support. A 'follow me' print arrangement should be setup which allows the user to simply print to a single print queue. The user can then walk up to a MFD and either enter a code or use an ID card to identify themselves, the MFD will then print the documents out.

Trusts should ensure that printing defaults to black and white, with users having to manually over-ride the settings for colour printouts.

The system should include a Print Management System which should support / be configured to:

- Support integration into the Trust's chosen user directory
- Report usage for staff and students across the trust, also by school
- Enforce print limits / quotas as needed by the trust
- Scan to email function
- Easy MFD terminal interface for end user
- Allow printing from a Bring Your Own Device network (if in place)
- Support Windows, Apple (Macs and iPads), Google Chrome and Android

Classroom Audio Visual

Classroom teacher displays should be:

LED/LCD display

Minimum of HD resolution

Appropriately sized for the room (65" expected to be the minimum)

Multi touch

Integrated audio

Interactive where needed, any interactive software, licensed for the site/Trust and remote use by staff

Support a minimum of 2 x USB 2.0/3.0 ports

HDMI 2.0 port

VGA port (to support legacy devices)

Direct Wi-Fi connectivity (802.11ac minimum)

An appropriate bracket and fixings for the screen size and wall

Support for screen sharing using standard services (Apple, Google, etc)

Support centralised management tools to allow central updates and power management

Large-Space Audio Visual

It's expected that any supplier would need to visit the school to audit the space, meet with the school to confirm the school's requirements and design an appropriate solution. However, the following basic principles should apply:

- Networked for maintenance / monitoring
- No filters in any projectors
- Allow Airplay and mirror cast
- Support 2 x HDMI video & 3.5mm audio inputs
- Appropriate microphones / wireless mics should be provided as per the school's requirements
- 5yr warranty on all active equipment and the installation
- Suitable protective enclosure in accordance with the environment/alternative uses of the space

CCTV

It's expected that any supplier would visit the site to fully understand the Trust's / school's requirements and design an appropriate solution. However, the following basic principles should apply:

CCTV must operate within an isolated VLAN on the existing network infrastructure and utilise the built-in POE.

A new solution should be cloud based and support the following specification

- A single School account that can support multiple operational units (OU) for each academy
- Delegated access to each operational unit (OU)
- 90 days of footage retention
- Footage contains the date & time
- Functionality to export CCTV footage in a standard media format (i.e., mp4, avi, etc)
- Redaction of CCTV footage
- Send alerts via the web console or emails for any camera connectivity issues
- Ability to deploy software / firmware updates from the management console which can be automatically deployed or scheduled
- All hardware should be covered by a warranty for a minimum of 5 years

Access Control

Where possible all readers should be cabled back to the controllers, although for distance or logistical purposes some readers can utilise wireless.

Gate or door intercoms should be compatible and where possible utilise the school's network

The solution should be synchronised with the MIS system. This allows for cards to be deactivated once their record in the MIS is set as a leaver.

Visitor Management

- Resilient LCD touchscreen, with built-in camera
- Sign in system for Visitors / Staff / Students
- MiFare card support
- Support MIS for e-registration
- Fire register reporting
- Staff swipe in / out reports
- Central database for school staff
- Printing of cards
- Email notification to the visitor's host
- Integration into a central Trust platform for centralised management and reporting

Cabling Specifications

Copper Cabling

A minimum of Category 6A LSZH UTP 4-pair cable should be used in all cases, terminating to suitably rated patch panels and data outlets. All cabling should be supplied with a manufacturer backed 20-year warranty and certificate supplied on completion of the installation.

Full testing should be carried out to the Class E Permanent Link standard as set out within BS50173 & BS50174 within the last 2 weeks of the installation period and appropriate certification provided at time of handover. (e.g., 'Fluke Full & Summary' reports).

One cable should serve one RJ45 data socket, e.g., if a quad outlet is required then 4 cables (each being 4 Pair Cat 6) should be used.

Individual Category 6 copper cabling runs should not exceed 90m (not including patch leads at either end). Including the patch leads the entire length should not exceed 100m.

Data Outlets

Copper data outlets should be Category 6 RJ45.

Outlets must have clear, protected labelling (through the use of a plastic window).

Fibre-Optic Cabling

All fibre-optic cable must conform to OM4 standards for multi-mode fibre.

All fibre-optic cabling must be terminated within an appropriate breakout box with LC type connectors.

A primary fibre-optic link of 16 cores is required from each patch room (containing either a single or multiple cabinets) to route directly back to the data cabinets in the server room.

Cabinets and Security

Within the ICT Server Room provision will need to be made for 1 x server cabinets to be delivered and installed by the IT Installation Contractor after the data cabinets have been installed by the cabling contractor.

Data cabinets should house the patch panels and leave space to house the active network equipment. Refer to Appendix B for details.

Server cabinets require 2 x 16Amp mains power supply presented with "commando" type socket. It should be located above the centre of the cabinet position on the ceiling.

Data cabinets must have 19" adjustable mounting profiles, and be 42U in height, 800mm (wide) x 800mm (deep) minimum, with lockable side panels and combination lockable front and rear doors.

Data cabinets must allow a minimum of 150mm between the front of the UTP patch panels / fibre termination panels and the back of the Data Cabinet door when closed. This is to allow for the minimum bend radius of fibre-optic cabling.

Data cabinets must have at least 500mm clearance between the front and rear adjustable mounting profiles to allow for active network equipment to be mounted.

Data cabinets should not have any cables, cable ties or other items which invade or impede the space required by the active network hardware and UPS units (where required) which will be installed within the cabinet. The full depth and full width between the adjustable 19" mounting profiles in data cabinets must be clear of all obstructions.

Data cabinets will require a 16 Amp mains power supply presented with a "commando" type socket. It should be located above the centre of the cabinet position on the ceiling.

Data cabinets should be provided with 1 x 12-way vertical PDU without surge protection. If a UPS (uninterruptable power supply) is installed in the cabinet, the PDU should have a C14 connector, to 12 standard 3 Pin UK plug sockets (BS 1363). If a UPS is not installed, the C14 connector should be replaced by a 16 Amp commando plug.

Data cabinets should incorporate a fan tray, located at the top of the cabinet to assist ventilation. This fan tray should incorporate a minimum of 4 fan units.

Where multiple data cabinets are required within a single location then the cabinets should be securely connected together without internal side panels but retaining side panels on the outside extremities.

There must be a minimum access space of 800mm around all sides of the data and server cabinets (or connected series of cabinets) to allow for internal access from all sides and to allow for the opening of doors and installation / maintenance of hardware.

Data and server cabinets must be fully earth bonded in accordance with the manufacturer's recommendations and national standards.

All data cabling must be terminated within the data cabinets on suitably rated 19" patch panels.

Each RJ45 patch panel and fibre break-out box should be supplied with horizontal cable management facilities (1U in height) to facilitate managed cable access (see diagram in Appendix B).

Vertical cable management is required within the data cabinets on both sides.

All Server Rooms and adjacent ICT staff areas should be securely lockable complying with the relevant Access Control system and / or utilising a more traditional 5-lever lock mechanism (this is to protect against unauthorised access). The expectation is that this room is used for server & data equipment only.

Computer desk key suiting – all computer desks should be on a key suite so that there is one key per room.

Server room & patch rooms – should be on one key suite separate from the master key suite so that access to these areas can be controlled.

Server room & patch rooms – doors should not have vision panels.

The server room must be kept to a sensible operating temperature, using a suitable cooling/heating method, within the external design temperature of the building. The room must be kept at a maximum of 24 degrees Celsius (regardless of temperatures outside of the room). There should be no hot spots in the room.

The patch rooms must be kept to a sensible operating temperature, using a suitable cooling/heating method, within the external design temperature of the building. The room must be kept at a maximum of 24 degrees C (regardless of temperatures outside of the room). There should be no hot spots in the room.

Patch Panels

Patch Panels must be rated to a minimum of Category 6A standards.

Patch Panels must be supplied fully assembled by the manufacturer.

Patch Panels must be 24-port only, and therefore multiples should be applied where appropriate.

Patch & Fly Leads

Fibre-optic patch leads will be provided by the IT Installation Contractor to connect the active equipment to the LC fibre patch panel(s).

Cat 6A patch leads will be provided by the data cabling contractor to connect the active equipment to the UTP patch panel(s). The School's IT Team will confirm the quantity and lengths of these, for budgeting purposes, it should be assumed that 2 x 2m UTP Cat 6A patch leads will be required per terminated Cat 6A cable.

Containment

Power and data must be segregated in separate containment channels with any dado, vertical, floor, or basket trunking.

Primary containment shall comprise closed type / lidded galvanised, galvanised tray or basket type containment. Where contained in a ceiling void the requirement for lidded containment is negated.

Containment must be sized to allow at least 30% spare capacity for future expansion.

The containment must allow for the requirements for the stipulated minimum bend radius for Cat 6A and OM4 fibre-optic cables, as appropriate.

Cables installed in the containment shall, wherever practicable, be laid with the heavier size of cables at the bottom.

Separation distances must meet those specified in BS EN 50174. If BS EN 50174 is superseded, then the latest, subsequent standard should be adopted.

Labelling

A clear and concise labelling scheme must be deployed. This must provide unique identification of each port to each patch panel and cabinet. What is listed below is the recommended labelling scheme, however, alternatives will be considered, providing that every data point is labelled uniquely in the school and can be readily identified back to the correct patch panel port in the correct cabinet:

Each cabinet across the site should be given a unique letter of the alphabet beginning at the server room with cabinet "A".

Where multiple cabinets are in a room, the cabinets should be labelled left to right (when standing facing the patch panels), starting at “A”.

Each block of 24 patch panels within a cabinet will be given a unique letter per cabinet starting with the top block of 24 being labelled “A”.

Each block of 24 ports should be labelled up as ports 1 through to 24 (manufacturers numbering can be used if 1U 24 port patch blocks are used).

This will allow each port across the site to be uniquely identified with a four-character code.

For example:

- Port “AA23” is in cabinet A, at the top in the first block of 23 points, Labelled as “23”
- Port “BA09” is in cabinet B, at the top in the first block of 24 points “A” Block, labelled as 9 or 09
- Port “DD12” is in cabinet D, in the fourth block of 12 points from the top “D” Block, labelled as 12.

In all cases the following scheme should be followed:

- cabinets should be labelled left to right (when standing facing the patch panels), starting at “A”
- within each cabinet patch panels should be labelled from top to bottom, starting at “A”
- 48 port patch panels should show the manufacturer’s port numbering (i.e., 1-48)
- electronic labelling devices should be used.

Cabling Provision for Additional Equipment

Note: Additional information may be required for each site where any of these items are to be included now or in the future. This provides general information only and further detail may be required when some of these items are to be included.

Digital Signage

Digital Signage will generally be a large LCD television screen (‘display’) that will provide information at key locations around the site. Each of these devices will be connected back to an active hardware device that is providing the output for the screen. The device supplying the media will be attached to the network and will generally be situated in the server room or nearest data room to the display. In some cases, the device may be located at the rear of the screen.

The display will be in the form of 42in to 50in LCD TV displays which may be mounted on device specific brackets and will typically be wall mounted. Typical dimensions of a 50in display are: (WxDxH): 1350mm x 170mm x 800mm

Each display will be mounted at as high as possible from floor level, subject to clarification with the school. Note - If a suspended ceiling is to be fitted, then this will typically be at 2700 mm. If this is the case, the display should be fitted below the suspended ceiling.

Provision should be made for screens to be wall mounted.

Displays could weigh up to 50Kg including mounting brackets.

Each display will require 1 x standard data point and 2 x standard power points – all services should be presented above agreed location of the display.

In special circumstances, provision may be needed for external speakers – detailed requirements should, therefore, be discussed with the school IT Team.

Teacher Wall (incl. Interactive Displays & Teacher Desk)

The teacher wall is specified as the wall designated for locating the interactive whiteboard and, where possible, the teacher desk. Interactive Displays are input devices which work in conjunction with the teacher's workstation. The teacher's workstation will be located on the teacher desk, subject to agreement with the school. In order to deliver a robust and guaranteed service, the Interactive display and Workstation must all be connected via specialist cabling and therefore not be wirelessly connected.

The wall may need to be pattressed to support the weight of the teacher display

There should be appropriate containment / trunking to ensure the cables between the display and teacher workstation are hidden

The USB specification limits the length of a cable between full speed devices to a maximum of 5 meters. Therefore, the total length for any teaching wall USB cable runs (including any USB patch cables) must not exceed 5 meters unless USB boosters are deployed

IP Telephony

IP Telephony will provide for any voice calls required across the site and for access to voice mail and external PSTN calls where permitted. It does not provide for any legacy analogue devices to be connected such as modems, facsimile machines or non-IP telephones.

Each Wired IP telephone will require an RJ45 network point. Power will be provided via the RJ45 Network Socket. (PoE)

IP Telephones should not share an RJ45 socket with other equipment, where this is not possible the telephone handset must support an 'In' and 'Out' ethernet port such that a PC device can connect to the telephone, which will connect to a wall data outlet

Any DECT wireless base stations that are IP enabled will require both a power socket and RJ45 Socket.

Wireless Access Points

Each Wireless Access Point will be mounted at high level and will require a Cat 6A+ network point. The device will be powered by Power-over-Ethernet (PoE).

Exact location will be determined by a wireless site survey.

CCTV (Security) – External

External cameras will be connected to UTP Cat 6A+ data cabling provided in accordance with the details elsewhere in this document

External cameras will typically be mounted on the external facia of the building, connected to an internal data point located on the inside of the building adjacent to the camera

External cameras will be powered via a PoE connection to the closest network hub / server room

CCTV (Security) – Internal

Internal cameras will be connected to UTP Cat 6A+ data cabling provided in accordance with the details elsewhere in this document

Data points will be located adjacent to the camera locations

Network Printers / Photocopiers

Each of these items will require a Cat6A+ data point

Each of these will require the provision of 2 x power points

Power socket allocation associated with LAN points

Power will be provided for ICT peripherals as follows.

- Each Floor box will have 4 x 13Amp sockets irrespective of the number of Cat 6A+ data points
- Each Wall Cat6A data point will have 2 x 13Amp sockets
- Each Digital Signage Cat6A data point will have 2 x 13Amp sockets

Glossary

LAN	Local Area Network	UTP	Unshielded Twisted Pair cable
POE	Power Over Ethernet	PSTN	Public Switched Telephone Network
RJ45	Registered Jack number 45	MFA	Multi Factor Authentication
IP	Internet Protocol	FTTP	Fibre To The Premises
USB	Universal Serial Bus	HDMI	High-Definition Multimedia Interface
LCD	Liquid Crystal Display	LED	Light Emitting Diode
OU	Organisational Unit	SSID	Service Set Identifier
RADIUS	Remote Authentication Dial-In User Service	Gbps	Gigabits per second
SAN	Storage Area Network	DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol		

---< END OF DOCUMENT >---