ICT STRATEGIC PLAN

Learning Academies Trust

Version:	2.2		
Approved by:	Board of Directors	Ratified date:	11 May 2023

Chief Executive Officer:	Simon Spry, BSc (Hons), PGCE, NPQH, NLE
IT Operations Manager:	Luke Pollard, MBCS, RITTech

LEARNING ACADEMIES TRUST

CONTENTS

CHANGES

Policy date	Summary of change	Author	Version	Review date
05/12/2016	• Draft plan created.	Luke Pollard, IT Manager	0.1	05/12/2016
09/05/2017	• Strategic plan published.	Luke Pollard, IT Manager	1.0	09/05/2017
15/01/2021	• Rewritten to accommodate operational/strategic changes.	Luke Pollard, IT Manager	2.0	15/01/2021
21/06/2022	• Update to section 3, structure.	Luke Pollard, IT Operations Manager	2.1	21/06/2022
22/04/2023	• Update to encompass larger MAT with 18+ schools. • Improvements to security and compliance strategy. • Updates to implementation strategy and timeline.	Luke Pollard, IT Operations Manager	2.2	11/06/2023

1. STRATEGIC DIRECTION

1.1. Overview

This strategic plan formalises the existing work undertaken in our organisation, and the strategic direction that we are pursuing to modernise the infrastructure and services required to deliver a successful IT facility to our schools and wider community. Over the course of several years, this plan has undergone numerous draft revisions in-line with the current environment, challenges, and target audience. This latest version provides a concise overview of our strategy to support the continued expansion of our MAT, and changes in priorities to enhance our security and compliance in line with recent government issued guidance and changes to legislation.

Having built a comprehensive understanding of our schools' existing environment and challenges, the focus on modernising our IT facilities is crucial to ensure the continued operation and development of our schools. Over the past few years, we have inherited several aging or non-functioning computing facilities and have spent a significant amount of time to correct and implement basic/fundamental facilities that were simply not present or functioning.

The trust has heavily invested in various technologies that enabled us to build a centralised facility that is efficient, effective, and delivers the resources required for our schools to operate. We have made significant progress by implementing numerous technical enhancements, and most importantly migrating all current schools into a single trust-wide Microsoft 365 tenancy. This has already proven to be invaluable for our users as this has enabled tools that have improved communication, collaboration, and delivery of education across the entire trust. Additionally, the integrated nature of our centralised infrastructure has eased a significant number of operational pressures from our Education, Finance, HR, IT, and Estates services.

Whilst to date we have made substantial progress in centralising our facilities, we must remain aware that we are comprised of several schools, each with their own identity and requirements. Our strategy is designed to provide a model that is fit for all and can adapt to any unique requirements when necessary. It is also important to recognise that as a large organisation there are some areas of our model where it is essential to implement a standardised approach to provide economies of scale, operational efficiencies, and improvements to our security and compliance.

Our priorities continue to focus on delivering improvements, and our current facilities are only the beginning of our journey towards ICT excellence. Much of our historic work has been reactive to ensure every school in our trust had met a baseline in order to operate. Since then, we have matured our IT services in line with principals established in the ITIL framework which has enabled us to operate proactively across the trust. We have a clear direction and strategy that provides an effective solution and service that delivers on efficiency, affordability, reliability, security, compliance, continuity, and scalability. All of this is surrounded by a 'continuous service improvements' process to ensure we regularly review the suitability of our strategy and to improve upon the delivery of our service.

In the following document you will find an overview of our strategy to modernise our IT facilities, services, and operation, to provide a solution for the challenges and demands present in our modern world. Everything presented in this document aligns to the beliefs and values set out at the inception of our trust, and ultimately aims to build upon those beliefs to further develop and improve the overall success for our staff, pupils, and community.

1.2. Delivery

The key to the successful delivery of this strategy is clear management, procedures, and transparency across our entire trust as we plan, develop, and implement changes. Historically, the trust has implemented several projects outside of any change management process due to limited resources and critical underlying issues that needed to be urgently addressed. We have since moved away from a reactive model and implemented a proactive model that ensures key stakeholders are thoroughly involved in the design, development, implementation, and improvement of any new or existing services/facilities.

From the inception of the trust, we have been working with our leadership teams to facilitate an open discussion and understand the current position of IT within our schools and the steps needed to move forward. In 2020 the IT Operations Manager held a conference day with all headteachers to engage in a transparent conversation around the deteriorating state of IT facilities within the individual schools and steps required to remediate this.

Figure 1-1, Learning Academies Trust, ICT conference for headteachers in October 2020.

During this conference he explained the complexity of IT operations, security, and compliance, emphasising the need for significant investment to ensure the infrastructure and services remained secure and operational. Headteachers left with an understanding of the technologies required to facilitate their schools' and how investing now would ultimately enhance the delivery of education. By holding these transparent conversations, we are working together to implement changes that provide value and improve the overall functions of our individual schools and trust.

Following the conference day, we have met individually with each headteacher to understand the individual ideas, challenges, and request from each school and have since used this information to formulate this strategic plan and to devise an appropriate ICT budget for each school. Throughout each meeting we developed a clear understanding of the current state of technology within their school and what is required ensure the school operates effectively. Once all parties are in agreement, we centrally manage the delivery of all ICT projects, budgeting, upgrades, security, and compliance requirements in order to effectively implement and maintain the infrastructure going forward.

Overall the planning day with all headteachers has been crucial in highlighting the scale of an effective ICT operation, and some of the ever-changing advancements within the industry. Throughout a number of conversations there appears to be a gradual shift of mindset and understanding that ICT should be seen as an enabler for the school and not just an expense; Something that has previously been highlighted in a Kreston academies benchmark report.

From our opinion, we believe the following graph provides an accurate representation of the current perception of ICT across our trust. Our leadership teams understand and embrace the need for technology and are welcoming to the changes required, however we believe there is a hesitance in viewing it as an enabler until the new technologies are thoroughly embedded into the classroom and making a visible impact for our pupils. Once the infrastructure is thoroughly embedded, we will focus on training our staff to utilise technology effectively within the classroom in order to harness the power and enhancements that collaboration and technology will provide to our schools.

1.3. Our approach

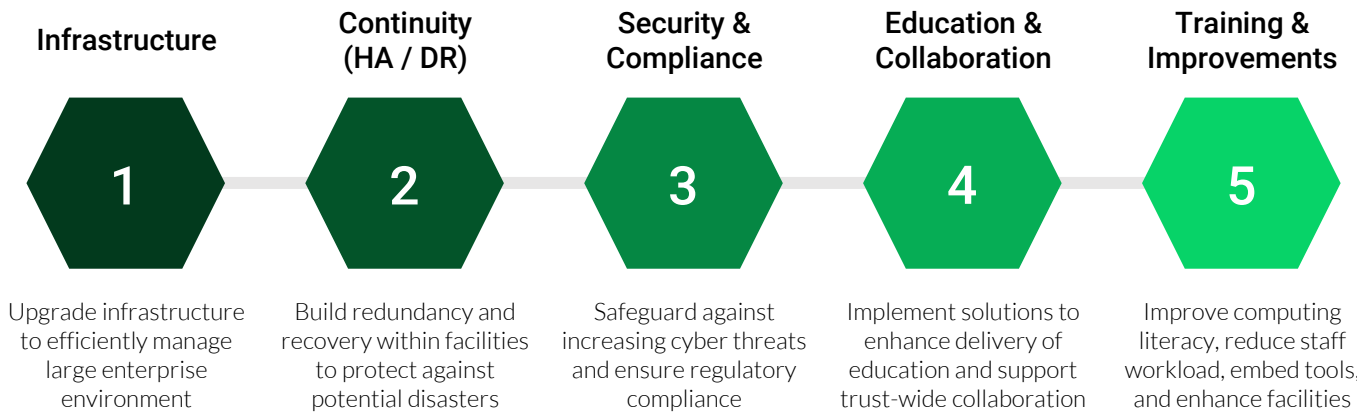
Under the local authority model each school was operating independently and as a result we had inherited several high-risk systems that were mostly outdated and inadequate. Having since reviewed the facilities in each school, we have implemented a centralised environment to support a range of modern technologies, with the option to adapt to individual challenges, and scale when additional capacity is required. For the most part, our schools are using the same systems for their software, services, and devices, with some niche projects implemented in a few areas.

As a trust there are clear operational and financial advantages in merging the infrastructure and managing the service centrally. It reduces the overall burden on schools to manage independent systems and ensures the future of their infrastructure is efficient, compliant, safe, reliable, and sustainable. Our internal IT team has a holistic view of the trust and can focus on the specific operational needs to progress our facilities and provide value to our schools. Unlike some external providers, we are not driven by profit. Our centralised service is here to improve the operation and compliance of our schools and focuses on providing value by optimising business processes, reducing costs to invest back into our schools, and developing an innovative facility to enhance the delivery of education.

This strategic plan was developed by auditing our existing environment and reporting upon the technologies and investments required to modernise our facilities. The plan was then subjected to an external quality assessment before being ratified by our Board of Directors back in May 2021. Since then, we have begun investing in resources to transform and improve our schools and we continue to deliver an environment that is increasing our operational efficiencies and improving the delivery of education for our pupils, staff, and community.

1.4. Implementation

Due to the scale and complexity of implementing a centralised enterprise-grade facility from the amalgamation of multiple independent organisations and environments, the overall strategy is broken down into five key phases.



Each phase targets a fundamental area of our infrastructure and services that will enable us to successfully deliver the improvements set out in this strategic plan. Upgrading our environment in this order will enable us to build a strong foundation to develop the remaining phases; For example, building the correct infrastructure in phase one allows for the seamless implementation of continuity, security, and compliance requirements in the later phases, and will ultimately improve the user experience and adoption of services in phases four and five.

A summary of the five phases are shown below, explaining the objectives of each phase and their relevance to the development of our infrastructure and services.

Infrastructure
Phase 1.

The infrastructure phase is the largest, most complex, and most expensive phase of our implementation. This consists of upgrading all legacy hardware and software and migrating all schools into a unified solution that is productive, secure, and scalable. Almost every piece of hardware inherited from our schools have been out-of-date and must be replaced with modern equipment; We are also migrating all legacy data and applications into a modern interconnected environment with our other schools across the city.

With a shift in the IT industry to utilise cloud based solutions, we are implementing a hybrid environment that utilises the benefits of both local resources and cloud based resources to deliver a modern infrastructure and architecture capable of managing thousands of users and devices. To enable a seamless experience for our users, we are also investing in a high speed and redundant internet connection to ensure every school can

facilitate uninterrupted access to resources. This allows for large number of users to access online resources simultaneously and enables schools to utilise various cloud-based software-as-a-service solutions, and our hybrid server infrastructure hosted at independent primary and disaster recovery site across the trust.

For identity, device, and application management we are utilising Azure AD and Intune services to unify the security and management of our assets. We have implemented various single sign on (SSO) and mobile device management technologies to manage and monitor accounts and devices from all vendors, provide a seamless user experience, and increase the security and compliance of our information assets and physical assets.

Overall, implementing the technologies listed below is critical to the successful delivery of phase one and the remaining phases.

- High-speed internet connectivity
- Compliant filtering and monitoring solution
- Secure networking equipment
- Adequate wifi coverage for speed and density
- Device management solution
- App management solution
- SaaS/PaaS/IaaS (e.g., Arbor, PSF financials, Microsoft 365, Google, Apple, Adobe, etc.)
- Centralised servers (hybrid)
- Centralised facilities (access control/CCTV)
- Secure, fast, compliant computing hardware
- Operational classroom hardware, e.g., screens

This is a complex phase as migrating multiple legacy environments into a modern central environment whilst keeping the schools operational is logistically and financially challenging. However, once all users and devices have been migrated into this unified environment, we will utilise technologies and automations to improve our operational efficiency, security, and compliance; Enabling our small central IT team to support thousands of users and devices across multiple sites without an exponential increase in staffing capacity or costs.

Continuity (HA/DR)

Phase 2.

The continuity phase ensures High Availability and Disaster Recovery solutions are implemented within the infrastructure to ensure the organisation can continue to operate during routine maintenance, or in the event of a failure or disaster. With 18 schools and 7,000+ users as of 2023, it is crucial that all critical infrastructure has appropriate redundancy so the entire organisation can remain operational.

For High Availability, all core infrastructure will have a redundant facility in place. The internet connectivity for each school will consist of diverse fibre connectivity through independent supplier infrastructure, supported by redundant ISP routers using HSRP, and redundant Smoothwall firewall/filtering appliances. The sites containing our primary and disaster recovery infrastructure are geographically diverse (across the city) to be supplied via different fibre exchanges and power distribution areas.

All critical services hosted on our central infrastructure will be clustered or load balanced dependent on the requirements of the failover technology; Our primary server room is supplied by multiple power phases and UPS equipment to reduce risks of a power supply failure. This allows our services to remain operational in the event of an environmental, logical, or hardware failure. High availability also enables our technicians to take servers offline to maintain our infrastructure and apply security updates without disrupting live services.

For disaster recovery, all critical infrastructure and services will be hosted in two diverse locations to protect against any natural or man-made disasters that may impact our ability to provide an operational service to our schools. A disaster recovery plan will be produced with appropriate procedures and technical redundancy to ensure our estate and facilities are protected against any event of power failure, flooding, fire, theft, terrorism, or other disaster that would otherwise prevent the schools within our trust from operating.

Security & Compliance

Phase 3.

The security and compliance of our organisation is paramount and has become the core focus of our work. Our schools hold high-value sensitive data for thousands of adults and children and have access to large amount of public funds. Due to their historically poor security practices, school systems were easy to exploit for financial and information assets making them a valuable and prospective target to attackers.

We are centralising our infrastructure as per phase one to protect against various cyber-attacks, moving away from a 'walled garden' security model to a 'zero trust' model instead. We have thousands of devices that work across multiple sites and outside of the trusted network perimeter, so moving towards a zero trust architecture relies on carefully managing the secure authentication and authorisation of all user and device identities.

Additionally, we are implementing a least privilege model across our infrastructure to ensure users are only granted the authorisations needed to perform their function. From network restrictions, admin privileges, resource privileges and more, the aim is to reduce an attacker's ability to move laterally across our network to prevent access to additional resources should they successfully breach part of the infrastructure.

Not only are we improving the proactive defences of our systems, but we are developing appropriate response procedures should an attacker breach our security measures. With the planned enhancements to our security, we will implement a Cyber Incident Response Team (CIRT) and Cyber Incident Response Plan (CIRP) to respond to an active attack against our facilities. This includes developing playbooks, simulating incidents and response procedures, implementing SEIM solutions to gather and correlate attack intelligence (such as syslogs, network intrusion detection systems, auditing logs, etc.), and meet regularly to review and improve procedures.

This work is complex yet critical to the safety of our users and the integrity of our trust. Recently the 'Meeting Digital and Technology Standards in Schools' guidance has been published by the DfE aiming to improve cyber security standards. This guidance is useful for setting a baseline that schools should aim to achieve, however we want to go further and are working towards achieving the CyberEssentials+ certification issued by the National Cyber Security Centre. This will provide an external audit of our security practices to ensure we meet the standard and once achieved will demonstrate our commitment to protecting our organisation and assets.

We are already well underway to achieving these standards, however there is still work remaining to ensure every aspect of the certification can be achieved and maintained. Over the next few years our aim is to achieve compliance with all requirements set out in the 'Meeting digital and technology standards', and to have the entire organisation certified with CyberEssentials+ and the SWGfL 360safe online safety accreditations.

To improve our compliance, there are systems that coincide with our security controls to help us achieve compliance with the General Data Protection Regulation and KCSIE filtering and monitoring requirements.

The implementation of Smoothwall will enable us to accurately filter and monitor individual staff and student devices no matter what operating system is in use or where the device is located; The key-logging facility also identifies safeguarding concerns that would not normally trigger via monitoring internet activity alone. This solution is an integral part of our digital safety strategy to reinforce our ability to safeguard and protect users whilst they are using our systems online.

For GDPR compliance, there are additional solutions embedded in our cloud security systems that we plan to implement to enhance our existing controls which will protect and monitor data stored within our facilities and retain control of all data shared internally and externally. This includes technical controls to prevent data loss or exfiltration and maintain the segregation of sensitive data within the organisation. Our priority is to migrate every school to our central environment so we can implement solutions to automate the retention and storage of data and guarantee the accuracy, security, and compliance of data held within our facilities.

Education & Collaboration

Phase 4.

The education and collaboration phase encapsulates the integration of tools and resources across the trust to plan and deliver education, increase collaboration by sharing best practice between professionals across the organisation, reduce staff workload, and improve pupil attainment. Phases one to three of this strategic plan focus on providing a stable and secure environment for our users, which allows for phases four and five to build upon the infrastructure and deliver tools to improve our staff and pupils experience and outcomes.

Already staff across the trust have started to utilise Microsoft 365 collaboration tools such as Microsoft Teams, Sharepoint, Yammer, etc. and are working together across the city to produce shared curriculum, resources, and planning materials. This is an invaluable resource as this provides an opportunity and gateway for staff to collaborate with other colleagues across the organisation to share ideas, opinions, and experience. Whilst staff have already begun to use the facilities of their own accord, an objective of phase 4 is to develop a campaign to increase adoption by encouraging all staff to utilise the collaboration tools to improve communication and collaboration within their own teams, as well as the wider trust.

Microsoft 365 also has a selection of tools that assist the delivery of education, the collection of and tracking of pupil's work, and various facilities to feedback and improve the engagement between pupils and their teacher. Utilising these tools can enable teachers to provide every child with realtime feedback and targeted learning materials to support an enriched and engaging curriculum. Microsoft continue to add and improve the tools within Microsoft Teams that allow teachers to create assignments that include automating and reviewing the reading progress of every child, tools for marking and tracking progress of allocated work, tools for delivering repeat and targeted lessons, tools to developing the programming curriculum, and other curricular tools such as Minecraft for Education which provides a catalogue of lessons and teaching plans for different subjects.

It's worth noting that we are not restricted to Microsoft solutions as there are several academic tools available from other vendors that we can also embed to bring benefits to our education delivery and operations.

The primary objective of phase four is to collaborate with our schools and integrate new tools that can support and develop the curriculum and operations using unified and modern technologies to improve outcomes. This will involve the ongoing cooperation of various teams across the organisation to evaluate and embed tools that aim to enhance the delivery of education, improve collaboration, and reduce operational inefficiencies.

Training & Improvements

Phase 5.

The training section of phase five will ensure we provide enhanced training and certification for all our staff to utilise the tools and environment to its full potential. Our central helpdesk are already developing articles that provide 24/7 access to self-help; However, we want to improve on distributing guidance and instead provide full training packages to help improve our user's digital literacy and confidence when using technology. There is a small number of staff who excel in utilising technology, but there is a large proportion of our workforce that only know the basics to perform their essential functions as they do not understand how to utilise other systems to support their lessons or to make their work more efficient.

Throughout this phase we will develop training video packages and internal certifications to encourage staff to improve their technical skills on a wide range of technologies. Alongside our internal training there are official and free Microsoft training courses for educators to learn the various Microsoft 365 education tools available. Additionally, there is potential for video training courses we create to be utilised as part of PTSA's materials offered to external clients to generate income back to the trust.

Finally, the improvement section of phase five will focus on a continuous programme of reviewing our existing infrastructure and services and gathering feedback from users in order to improve the overall experience and effectiveness of our environment. This process is part of the continual service improvements cycle defined in the ITIL framework and will be an ongoing endeavour to review our service strategies across the organisation. If appropriate, we will update our strategies to implement any operational or financial efficiencies identified.

To enable our team to deliver the required facilities and services successfully and efficiently throughout these five phases, all operational and infrastructure decisions will be governed centrally by the trust. Individual requests for resources will be agreed upon in consultation with the school(s). As we improve our change management process, many of the decisions will be reviewed, assessed, and agreed with the relevant experts, guidance, and input from key stakeholders. Decisions that are authorised at a trust level will always be in the best interest of our schools, and where any major project and investment is involved, the Board of Directors will seek external quality assessment to ensure the advice given from our internal teams are appropriately reviewed and approved by other industry experts.

1.5. Timeline

At the time of updating this document (April 2023) we have made excellent progress with our existing plans and now must adjust our timeline and priorities to consider the nine new schools joining the organisation. The timeline below is an estimated time to complete the remaining upgrades and onboarding of our new schools.

2023 Q3	- Completion of security policies and technical controls - Amendment to backup strategy and increase retention - Central servers, new hardware infrastructure installed - Trust-wide telephony systems migrated - High View Migrated - ICT Office moved to new building
2023 Q4	- Central servers, all virtual machines and services installed - Central servers, retire legacy hosts - Horizon, migrate central MAT resources - Horizon, communication strategy implemented - Horizon, inducted to our central LAT service desk - Horizon, access, and documentation received from provider (TME) - Full audit of Horizon infrastructure, cloud tenancies, and data
2024 Q1	- Present ICT strategy and budget to Horizon headteachers - Plan budget for each school (to implement September 2024) - Plan migration of each school - Begin setup of resources e.g., DNS, firewall, data migration, etc. - Begin installation of leased lines & Smoothwall
2024 Q2	- Migrate Horizon school #1 - Migrate Horizon school #2
2024 Q3	- Migrate Horizon school #3 - Migrate Horizon school #4
2024 Q4	- Migrate Horizon school #5 - Migrate Horizon school #6
2025 Q1	- Migrate Horizon school #7 - Migrate Horizon school #8
2025 Q2	- Migrate Horizon school #9

With such a significant expansion to the organisation this timeline will be reviewed regularly and is subject to change dependent on any challenges that arise over the next year. This timeline represents an indication of the projects ahead and will be updated once we have accurate information on the condition of Horizon's existing facilities.

2. INFRASTRUCTURE AND SERVICES

2.1. Overview

To implement our ICT strategy and provide an effective solution, there is a clear necessity to modernise the existing infrastructure to support the current and future demands of technology. Our legacy infrastructure is provisioned on premises using equipment and strategies that have quickly become outdated. We must recognise the value of IaaS, PaaS, and SaaS (Infrastructure, Platform, Software as a Service) solutions that can complement our hybrid facilities and replace our legacy infrastructure to provide major efficiencies and improvements across our entire ICT estate.

In the original draft of this strategic plan, we evaluated moving entirely to the cloud to reduce the costs associated with local resources, however after reviewing the strategy we have decided to move forward with a hybrid approach due to the hidden costs which when calculated would have costs exponentially more. Our hybrid approach allows us to utilise both as-a-service cloud solutions and locally hosted solutions to best facilitate our organisation and keep operational costs to a minimum.

With a mixture of local and cloud-based resources, detailed in this section you will find our strategic concepts and decisions that support the implementation of a modern infrastructure and allows for automations and operational improvements to provide a secure, efficient, and effective computing environment for our users.

2.2. Choosing the Microsoft 365 environment

When working in the education sector, the choice of cloud platform is either Microsoft 365 or Google Workspace due to the educational tools integrated within the platform. Now the historic challenge for any leadership team is whether to adopt the Google or Microsoft route and understanding what platform is better for their schools. Whilst this has been a debated topic across the industry, we have chosen the Microsoft 365 route for a variety of reasons.

The key to making this decision is looking holistically at the entire platform and the additional tools it provides in addition to the classroom tools used for education. As important as the teaching tools are, if users are unable to seamlessly onboard with the platform because the existing infrastructure does not adapt well, then the user's experience is hampered and can become an obstacle when trying to onboard to a new environment and process.

From the perspective of systems administration, the Microsoft 365 platform wins without question. For a small to medium business, we would argue Google is much simpler to setup. However, when operating at an enterprise scale with multiple sites and systems, Microsoft gives us granular control over the entire infrastructure to allow flexibility on how we choose to deploy, configure, protect, and utilise our environment. With several thousand user accounts, having everything in one place is far more efficient to manage and maintain.

When it comes to integration, Microsoft 365 provides multiple tools that offer flexibility and compatibility with most online platforms. Having the ability to synchronise, provision, and implement single-sign-on to third-party services drastically reduces the time and resource required to manage them, and provides a much cleaner, user-friendly experience. Through API automation and integration, we can improve the accessibility and reliability of services for our users and reduce any risks of introducing errors into the system through manual data-entry.

Microsoft 365 also provides an exceptionally powerful pre- and post-breach enterprise security facility that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications. This provides enhanced protection against sophisticated attacks and helps us to keep data secure and compliant. As we continue to improve our organisations security processes, these tools facilitate the required technical controls to keep our users safe and enable our trust to achieve compliance with the NCSC CyberEssentials+ certification.

From a user's perspective I can understand that when you first look at Microsoft 365, it can be overwhelming with the sheer quantity of tools available. There are so many astounding tools that will support with our education and operations, but often users do not know what they are, what they do, or where to find them. As part of our efforts to simplify access to our facilities, we have developed an intranet portal that seamlessly integrates with Microsoft 365 to guide users to the plethora of resources available (both in Microsoft 365 and across the web). Having spent the time to ensure the user experience is simple and seamless, the rollout across the trust has been a success.

The final element of the Microsoft 365 suite that completes the package is the Microsoft Teams collaboration and classroom tools. One of our trust's core beliefs is schools work best when they work together, and even before the global pandemic occurred, we were working towards implementing a platform that enables our staff to share resources, ideas, and best practice with other school across the trust. Teams became our platform of choice, as it integrates directly with our file sharing system, video and messaging systems, and other services to facilitate the collaboration between staff across the organisation and integration of quality educational tools for our pupils.

In addition to collaboration, the pandemic has accelerated our implementation of the assignments and online learning features within Teams. Our teachers have already spent thousands of hours providing live lessons and have assigned hundreds of assignments to our pupils. It is a superb tool to support teachers at home and in the classroom. Teams is not just about remote learning as it provides an online learning platform that improves the interaction and communication between staff and pupils. The tools can be utilised throughout the normal school day for individual or group work and will provide a whole new method for learning and increasing engagement in the classroom.

2.3. Choosing our endpoint architecture

When looking for an appropriate solution to operate the whole of our infrastructure, there were several avenues to investigate to ensure we picked the correct tool. As part of this process, it was imperative that we keep up to date with this rapidly changing industry, as one of the driving factors behind our choice is due to the global migration toward cloud and mobile driven technologies. Whilst there was good evidence to approach this with a tried-and-tested environment such as a Windows domain with traditional thick clients, or hypervised Citrix / RDS farms using a thin client model, we chose to move toward the emerging MDM/MAM model to enable cross-platform compatibility with our current devices and any other devices and operating systems we may see in the future.

Is this still the right choice? In our expert opinion, yes. When we first looked at a hybrid environment with MDM (Mobile Device Management) and MAM (Mobile Application Management), the tools necessary to operate an entire infrastructure were not readily available. Instead, they were actively being developed by leading software vendors and companies such as Microsoft. Move on several years and we now have sophisticated and mature tools available for us to provide enterprise authentication, file storage, device management, app deployment, security controls, communications, printing, and more. Unlike the other solutions, an MDM/MAM cloud driven environment can manage various operating systems including Windows, iOS, MacOS, Android and ChromeOS. This is crucial as we continue to build a solution that can support all the individual technologies available within each school.

Furthermore, to support the choice of MDM/MAM; If you look at the latest industry changes in the CPU market and try to draw between the lines, it appears that a new processor architecture will be favoured in the future. Some key device manufacturers are starting to build their own silicon chips using non x86/x64 architectures, and whilst mass adoption is still a considerable time away, having a system capable of managing these devices in the future is crucial.

2.4. Network infrastructure

To enable us to manage our current infrastructure effectively and prepare for any new technologies, we are first focusing our efforts on upgrading the core network and connectivity that form the backbone of our infrastructure. We have already seen evidence of one of our schools unable to operate effectively by jumping ahead with modern technologies without first taking into consideration the connectivity requirements. As we start to implement these changes, we will first install a solid foundation for which the rest of the facilities will be built upon. In the sections below we detail the technologies being implemented to enable the successful delivery of our modern infrastructure.

Internet connectivity

Each school will be fitted with a 1Gbps leased line and a 100Mbps backup line. Where possible these will be installed by two different telecom suppliers to provide redundancy for our schools. The gigabit connection will ensure there is capacity to allow all users to access our cloud hosted resources quickly and concurrently.

Smoothwall filtering and monitoring

Having previously completed a tender exercise, we have chosen Smoothwall as our supplier. Each site will have two physical appliances to provide advanced filtering, monitoring, and UTM services. These appliances will be configured

as a highly available (HA) pair to facilitate redundancy of their internet services. This solution also includes a cloud service that enables us to filter and monitor devices off site, something we have previously been unable to do.

Furthermore, Smoothwall provides a significant improvement to safeguarding with tools that proactively identify and alert our safeguarding leads to any serious incidents or trends that require intervention to protect our users.

Enterprise switching
We will replace all consumer/low-end network switches with high-quality enterprise switches. Whilst there is an initial investment, these switches provide a significantly higher throughput and several critical features required to effectively operate and secure the network.

Enterprise wireless
We will replace all wireless systems at each site with enterprise access points using Wifi-6 as standard to provide consistent capacity for an entire classroom to access resources simultaneously. Each site will receive a professional heat map survey which will determine where the new access points are to be installed, ensuring appropriate coverage and throughput for a minimum of 32 devices in each teaching room.

2.5. Cloud infrastructure

Our cloud infrastructure expands across multiple platforms and consist of services from a variety of vendors. Some of them are granted to educational establishments for free, while others require payment. Many are provided within Microsoft 365 and Azure already, with a few additional services sourced from third-party vendors.

Network management
Network device (access points and switch) management will be provided by the Aruba and Cisco cloud controller services. This allows for the automatic provisioning and monitoring of all network infrastructure and connected client devices. Our firewall and proxy appliances are managed via our local Smoothwall appliances.

Email, communications, and productivity
Email services are provided by the Microsoft 365 platform through Microsoft Exchange and Exclaimer. Collaboration and productivity tools are provided by Microsoft Teams and Microsoft Yammer (Now Viva Engage).

File storage
All data will be served via Sharepoint and Onedrive. The data hosted online removes the requirement for remote access through VPN/RDP connections and improves accessibility, data protection, recoverability, and auditing.

Device and application management
Our chosen device and application management platform is Microsoft Intune, as it is native to the Microsoft 365 platform and optimised to manage Windows environments. Intune is also capable of managing iOS, MacOS, Android, and ChromeOS environments too, with facilities to enable federated SSO integration with other resources.

The majority of our Windows and iOS devices are already managed by Intune and we are utilising Windows Autopilot for app and device deployment. Having moved to Intune, we have seen a significant optimisation of our applications and device deployments and our objective is to migrate all remaining devices onto Microsoft Intune.

Identity management
User identities will be managed by local AD servers, Microsoft Azure, Apple School Manager, and Google Workplace. These are replicated identities linked via SSO to improve the security and user experience across our environment.

Security
All security software and processes will operate through the Microsoft Security Centre and Defender services within Microsoft 365. These facilities provide native tools for detection, prevention, investigation, and response capabilities across all endpoints, identities, email, and applications. This will be complimented with a SIEM to monitor any events and anomalies across our local infrastructure. (Security facilities are detailed in section 4 of this document).

Web Hosting and DNS servers
Our web servers and DNS hosting are currently provided by Krystal Hosting Ltd. This is a trusted UK company which provides a reliable and affordable solution for hosting our websites and serving our public DNS.

2.6. Local infrastructure

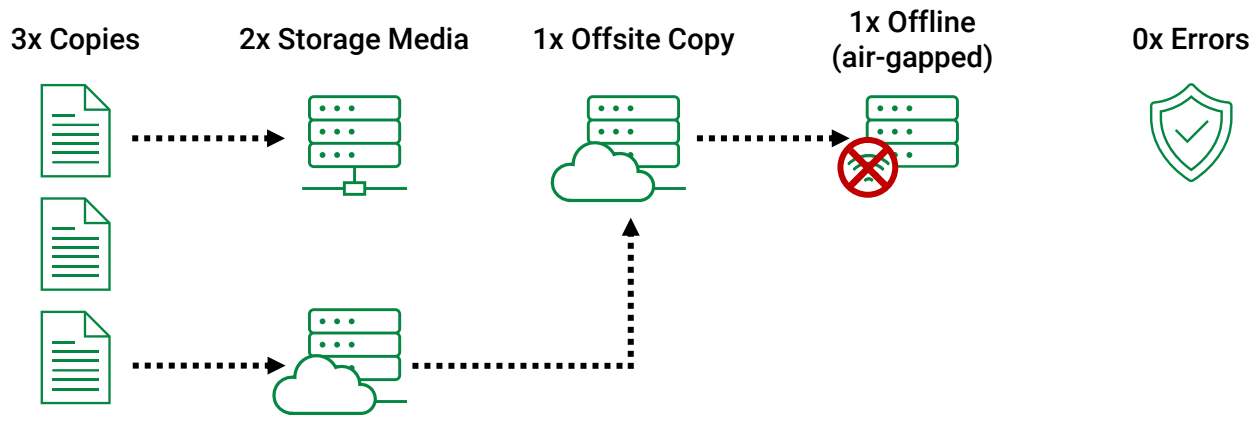
Servers
In the original draft of this strategic plan we evaluated moving our server infrastructure to the cloud, however after reviewing the strategy we have concluded a hybrid approach has a lower total cost of ownership and will better facilitate the requirements of our organisation at this stage. We have recently upgraded our server hardware to increase capacity and performance for the entire trust; This includes a primary site hosting core infrastructure and secondary site hosting disaster recovery infrastructure.

Throughout the design of our infrastructure, we have allowed for high-availability (HA) and disaster recovery (DR) solutions to ensure the infrastructure remains operational. Central servers will be securely maintained and deliver core authentication, authorisation, certification, filtering, telephony, printing, monitoring, remote support, and access control services using the following technologies:

- Domain Controllers, Azure AD Connect, NPS, DNS
- Certificate Authority, NDES, SCEP
- Print Server, PaperCut MF, Print Deploy
- Telephony
- Web Hosting
- SQL Database Server
- PRTG Monitoring
- Remote Support
- Paxton Door Access
- Network Load Balancing
- Automation (Powershell, REST APIs)
- Windows Updates (WSUS)

Without publishing the technical details in this document, the implementation of these technologies allow for improved management and increased security of our network. Any remaining local servers hosted within schools will be decommissioned to ensure we can secure, monitor, and maintain all services operating within our infrastructure.

Backup and recovery
As large organisation with over 7000+ users as of 2023, we have several terabytes (TB) of raw data to store and multiple different sources of data to backup including local servers, hosted services, and Microsoft 365 data such as emails, OneDrive, Sharepoint, Calendars, Teams groups, etc. To protect our data, we are implementing multiple local solutions to provide a 3-2-1-1-0 backup strategy for our organisation. This entails 3 copies of data, stored on 2 different media types, with 1 copy offsite, 1 copy air-gapped, and 0 backup errors.



After evaluating different licensing and storage solutions and their associated costs, we have chosen a locally hosted system that enables various backup solutions from various sources such as SFTP, software agents, and hypervisors. We have implemented multiple storage appliances at different sites to facilitate the media and offsite requirements of the strategy, with an additional storage media that facilitates the air-gapped backup. This resource currently has storage available to provide adequate retention of our data, however we have the option to expand the appliances to increase capacity if required at a future date.

2.7. Hardware: rolling programme

What is prominent in the industry today is the speed at which technology is being developed, released, and then becoming outdated. Due to the ever-increasing demands of modern technology and the continuous fight against cyber security threats, the hardware required to operate the latest operating systems and software updates often require additional resources to remain compatible. In several instances across the trust, we have devices that do not meet the minimum supported specification (OS version, TPM chip, processor) and will need a replacement.

Having reviewed the current IT estate, we have a vast range of hardware in use with limited conformity across the age and specification of devices. The majority of computers have been replaced over the past five years, however many of the earlier replacement devices are starting to deteriorate due to their age and lack of rolling programme. There are also a number of infrastructure devices that are incompatible with new security updates, leaving several vulnerabilities across the network and devices that are not stable when performing configuration changes.

Looking at this legacy model, schools would historically purchase new equipment and keep it running until it either ceases to function or breaks beyond economical repair. As a trust we cannot continue to operate in this way as this often leads to significant downtime, unplanned expenditure, and continues to pose a security risk to all our users. This IT strategy will move our schools away from this one-off capital expenditure mindset and will implement a full rolling programme that ensures all equipment is refreshed on a regular schedule.

By implementing this rolling programme and increasing the investment in IT, we understand that there will be an impact to the school budgets. Our modelling shows an initial peak in the first two years across every school whilst the core infrastructure is upgraded, followed by a lower stable budget thanks to the consistent ringfencing of funds for regular hardware replacement. Throughout this entire process we have made every endeavour to reduce any unnecessary expenditure and provide value for money through long term investment and bulk purchasing power.

2.8. Hardware: functionality

When planning and building our infrastructure, one of the key elements we have focused on is the interoperability of all software and hardware used across the network. There is a range of different computing technologies currently in use as they each offer their own advantage within the classroom, however they do not all work seamlessly with each other due to the current infrastructure unable to support all our different operating systems. Moving our data and infrastructure to a hybrid cloud architecture enables these technologies to work seamlessly together.

In providing a system that supports the use of different technologies, we give teachers the opportunity to innovative and provide new ways of engaging pupils in their education. We know there are a plethora of classroom focused tools available on other devices such as iPads, and allowing teachers to seamlessly access resources from any device will make a key difference in the adoption and use of technology to improve education.

Regarding the students, we have already seen the benefits of using cloud-based technologies throughout this pandemic by enabling a facility that can be accessed through a number of different devices. As we continue to migrate the rest of our infrastructure online and streamline the access to our learning resources, we hope to see these technologies further developed and embedded in schools and at home.

2.9. Account management

With the size of our organisation, having an effective account management procedure in place is essential to keeping the organisation operational. As we continue to move forward, many of the processes have already been or will be automated to ensure our users have a quick, consistent, and secure provisioning process that provides appropriate access to our computing infrastructure.

Our previous decision to migrate the MIS system to Arbor has been instrumental to these automations as we have direct API access to our data. When the school administrators make any additions or modifications to the pupil data, our fully autonomous scripts will provision and deprovision the relevant resources for each pupil. This highly efficient process enables our pupils to have immediate access to their resources and ensures they are correctly linked to their class; A process that is complex, but critical to ensuring their online learning platform is working effectively.

For staff accounts, we are in the process of developing a partially automated solution that will be initiated by the HR department through the IT service desk. This will ensure accounts are created with the appropriate permissions and all new staff are taken through a step-by-step provisioning and induction process. This provides a professional and inviting start for any new member of staff joining the trust, whilst ensuring the appropriate departments are informed and valuable assets are assigned/audited across the organisation.

2.10. Account integration

To ensure our systems are easy to access, our infrastructure has been setup to automatically provision Microsoft, Google, Apple, and Adobe accounts for every user. Each service has SSO (single sign on) capabilities enabled which allows for seamless authentication across all devices and online services. By enabling these features, we have greatly reduced the security risk associated with managing multiple accounts as the provisioning, deprovisioning, and access rights for each account are managed from one platform and propagated throughout the other services.

For our users this means signing into a device with one username and password that provides access to all resources without having to retype a number of different account details to gain access. In addition, many new websites have integrated a Microsoft SSO feature, meaning that you can login with a single click instead of signing up and having to remembering another password. Whilst this may not seem a significant issue, having an infrastructure capable of reducing the number of logins required will drastically reduce the amount of time it takes younger pupils to login and access their work, thus freeing up 10-15 minutes of each lesson for valuable learning instead.

3. ORGANISATIONAL STRUCTURE AND OPERATIONS

3.1. Overview

The following section details the strategic decisions that have been made since the inception of the trust and some of the planned changes to optimise the current ICT service, operation, and governance structures. Our primary goal is to ensure that we have an effective structure in place with appropriate capacity, expertise, and governance.

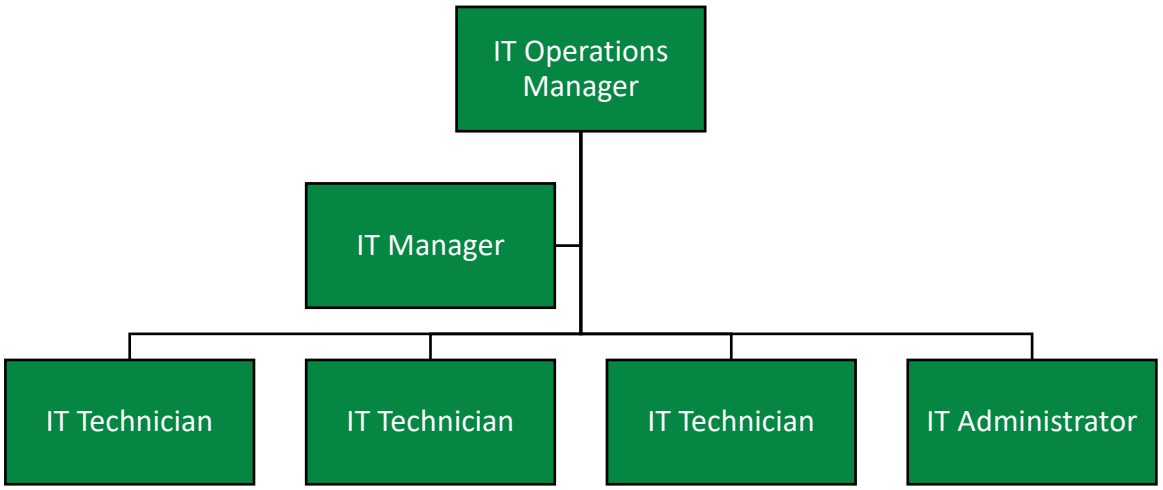
If we first look back to before the trust was formed, we had a model whereby two schools were supported by their local secondary school, two schools were sharing a full-time technician, and the remaining schools received support from external contractors. Whilst this model had kept the school functioning in the past, it became clear that was no long-term strategy for modernising IT due to a support model that had challenges in terms of the relevant skills and expertise required to drive them forward.

At this point early in the growth of our trust, we made a strategic decision to amalgamate our technical team and cease all external contracts. Over the course of a few years, we have been able to introduce a centralised service that has significantly improved our service efficiency and enabled a standardised approach to manage capacity, prioritisation, project planning, and the overall strategic direction. Our schools now have a single point of contact (SPOC) to our service desk, enabling our small team to handle a significant quantity of requests efficiently.

With the recent expansion of our trust from nine schools to eighteen, it is important at this stage to adjust our team to ensure the correct candidates are present in each role to provide the appropriate level of service to our schools. This new model aims to provide a higher-level technical expert who will support and provide redundancy for our IT Operations Manager to ensure the continuity of IT services within our trust, consequently reducing a significant operating risk to the trust at this time.

With the proposed change in structure, we have benchmarked several IT roles within the education sector across the UK to form a reference of current salaries within the field. To attract and retain any potential candidates for these roles, we have adjusted our salaries in line with the benchmarking report to account for the technical experience and skillset required from our employees.

The proposed structure for our central IT Department is displayed in the organogram below:



This structure is designed on having a smaller team with high level skills and aptitude to provide a cost-effective service to our schools. With several operational efficiencies and automations already in place, the team will provide adequate resources to manage eighteen schools.

Each position has delegated responsibilities, all of which are outline in the table below. This change in structure will enable our team to focus on the reponsibilities allocated within each role.

IT Operations Manager	- Supplier and contract management - Financial strategy and budgeting - Service continuity management - Information security and compliance management - Cyber security and response management - Risk management - Project management - Policy management (including SLAs, guides, handbooks, etc) - Resolution of service desk escalation - Line management for IT team
IT Manager	- Monitoring and reporting of infrastructure health - Incident and request management - Change management - Resolution of service desk escalation - Service asset and configuration management - Knowledge generation (creating documentation/self-help articles/training) - Proactive maintenance and infrastructure upgrades - Disaster Recovery and Cyber Incident response
IT Technician	- Monitoring of infrastructure health - Resolution of service desk incidents and requests. - On-site visits to resolve incidents, requests, and project works. - Proactive maintenance and upgrades - Knowledge generation (creating self-help articles/training)
IT Administrator	- Knowledge management (creating and maintaining self-help articles/training) - Asset management (recording and auditing of assets). - Data protection (compliance auditing and management, SAR management) - Data management (maintaining data within systems that do not support automated provisioning and deprovisioning) - Policy compliance (regularly review policies and manage compliance)

With a consolidated team to manage the entire trust, we will continously monitor and review our capacity to deliver our services. We have already made efficiencies through the use of automation to reduce the overall workload on the service desk and will continue to find ways to improve our ongoing operations and delivery.

The new IT Manager role will make a positive impact to our service desk and project delivery, as well as provide technical experience to help support and grow our existing technicians. The benefit of this model is the ease of growing and expanding our team, and our ability to adapt to new challenges or expansions in the future.

3.2. Roles

As the trust continues to grow and improve their services, having the appropriate technical support, administrative, and management capacity is crucial to facilitate the key roles defined below that will keep the organisation safe, compliant, and operational. These roles are allocated to individuals/teams as shown on the previous page.

Information security and compliance management

The role of information security and compliance is crucial in protecting our trust and ensuring we adhere to the appropriate privacy and security regulations within our industry. With access to highly sensitive information and providing facilities for children, we must ensure all systems and processes in use are safe, secure, and compliant.

Cyber security and response management

The role of cyber security and response management is imperative in designing the security systems, response strategy, and recovery strategy to protect our organisation and remain operational. This role will be responsible for implementing cyber security training and all administrative, physical, and technical controls required to protect the orgnisation and achieve compliance with the National Cyber Security Centre CyberEssentials+ certification.

Risk management

The risk manager is responsible for capturing and controlling all risks associated with ICT, ensuring the trust-wide risk register is kept up to date using a probability/impact assessment. This register is regularly reviewed by the board and must detail the actions taken to mitigate risks or the decisions for acceptance of risks.

Project management

With a significant number of upcoming projects, it is essential to have a project manager capable of communicating with suppliers and key stakeholders to ensure each project successfully delivers on time with the intended outcome.

Change management

The change manager is responsible for the planning, development, and monitoring of change management plans and activities including communications, training staff, key stakeholder management, change impact assessment, and change reinforcement. With the vast number of upcoming changes, this role will be essential in managing the transition for schools and ensuring minimal impact and disruption across the trust. As we look to improve our infrastructure and services, this position will play a vital role in keeping the organisation informed and operational.

Service continuity management

This role has responsibility for ensuring all key services have a continuity plan and a detailed procedure for recovery of any impacted service. There are already services across the trust that already have a solution for continuity in place, however these will all need to be thoroughly documented, tested, and reviewed.

Incident and request management

This role is to oversee the service desk and ensure all incidents and requests are appropriately logged, prioritised, and actioned. They will work closely with the support team to resolve outstanding issues and to design methods and procedures that aim to reduce the overall number of problems and incidents entering the service desk.

Supplier and contract management

The role of supplier engagement and contract management will prove vital to the trust as we move towards a model that encourages a partnership with our suppliers. In our centralised model we can build upon supplier relations that provide value to our schools by focusing on our business needs, streamlining the supply and purchasing of goods, validating the supply-chain, and providing economic value through bulk purchasing and customer incentives. This role will focus on building those relationships, negotiating contracts and service level agreements, and ensuring services, contracts, and purchases all meet the expected level of quality and value for our trust.

Service asset and configuration management

The manager for this role is required to keep an accurate record of the assets and configuration within our current IT estate, detailing any assets that may impact other devices or services. They will keep track of all assets to identify and log any change requirements. Most assets are already recorded within our configuration management database,

however there are a number of historic inaccuracies that need to be addressed along with the documentation of any relationships between assets. This role is crucial to developing an accurate database so that we can maintain our IT estate effectively.

Knowledge management
The role of knowledge management is shared across our entire technical team to allow the capture of knowledge that will enable efficient management of our infrastructure and services. The role of the Knowledge Manager is to govern the additions and modifications to our information and ensure that our team is documenting all changes, recording root analysis and resolutions, and contributing to the development of self-help guidance for our users.

3.3. Service desk

To standardise our procedures, we implemented a centralised service desk to provide a single point of contact (SPOC) for staff to raise all technical issues and queries. It has significantly improved the communication from our staff and has enabled us to keep an accurate log of all incidents and requests to ensure they are actioned efficiently.

We use the ITSM (IT Service Management) tool FreshService which includes a self-service facility for our users and provide our technicians with advanced utilities that will enable the management of projects, incidents, problems, change requests, knowledge, and more through a series of integrated ITIL processes. This software continues to improve and maintain our communications, monitoring, and prioritisation of tickets raised across all schools.

With our service desk in place, the focus moves to improving the customer experience and decreasing the response and resolution time of our service. Our team works incredibly hard to provide an outstanding service for our users and take great pride in their work, however there have been several historic tickets that have fallen far below an acceptable resolution time due to the previously reduced capacity in our team.

Our goal is to ensure users feel confident in raising a query and receiving a response or resolution within an agreed timeframe, or to have the knowledge and appropriate access to resolve an issue themselves through our self-help offerings. In order to reach our goal and provide a rapid and positive experience for our users, there are a number of steps we will take as detailed below:

Customer portal
The ITSM software provides a modern customer facing portal with seamless access through SSO and enables our users to access self-help options, to create new incidents or request, and to track their existing tickets.

In providing users with access to their ticket history we aim to build trust in our service by evidencing the quick response and resolution of their queries. Allowing users access to create new request and respond to existing requests should also encourage their engagement with our team in order to resolve issues quickly and efficiently.

We are also building a database of self-help articles to empower our users and encourage them to resolve their issues using the guidance available. This results in a faster resolution for their issues and in doing so saves valuable time and resources from our support team.

Service catalogue
As part of the self-help options, users will also have access to a number of predefined catalogue items in order to automate and streamline a number of processes. For example, a user should be able to request a piece of software or order a new ID card, mouse, laptop charger, etc. direct from IT without the bureaucracy involved in placing an order or accessing a service. Another use case is for requesting a routine process or tasks. For example, the HR team may complete a request form for a new employee, and this will automatically trigger a series of automated or manual tasks such as creating a new account, printing a new ID card, and purchasing the appropriate licenses.

By providing a service catalogue within the customer portal we give users a simplified procedure that enables the automation of a number of standard requests and approval processes. This provides an efficient and seamless process for the support team and ensures our users requests are actioned quickly.

Service level agreement (SLA)
When dealing with tickets, our technicians will triage the initial ticket and then the relevant team will respond as soon as they can. In some instances the user does not respond to the reply and the technician has not followed up on the request and therefore the ticket remains unresolved for longer than expected. With the ITSM software, there are a number of tools configured to automatically alert, highlight, and follow up on tickets to ensure they are dealt with promptly, and within the times set in the service level agreement.

With the ability to easily view and track these statistics, our incident and request manager will be responsible for reviewing any outstanding request and allocating resources within our team to chase up and resolve these issues.

Currently our central IT team do not specify an SLA with each school due to the complications and time consumption of migrating every school onto our central facilities. Once all migration work is completed, we will present schools with a defined SLA to provide a target response and resolution time for all tickets. This will help to build confidence in our support service and allow users to understand the agreed timeframe for tickets to be resolved.

Satisfaction surveys
To ensure that users are happy with the response they are receiving, the software sends a satisfaction survey at the end of each ticket. This allows users to rate our service and inform us if they are unhappy with the support they have received. This information allows our technicians to follow up with the user if they are not satisfied and allow the monitoring of KPI statistics to identify trends and address any concerns or outstanding issues.

Management reporting
With the additional reporting facilities available, we have a significant amount of data that will be used to review the current progress and status of operations across the whole trust. Analysing this data will enable us to improve our existing service and further develop efficiencies within our operation to ensure our users are receiving a valuable service. This data will also be used to report back to key stakeholders within the trust.

4. SECURITY AND COMPLIANCE

4.1. Overview

Learning Academies Trust is a large organisation of 7000 users (as of 2023) with access to a significant quantity of sensitive information of both adults and children. We have an obligation to provide appropriate security controls and procedures that protect our data subjects, assets, and finances. The National Cyber Security Centre, Department for Education, Education Funding Agency, and Information Commisioner's Office have published legislation, guidance, and campaigns for organisations to enhance their security and improve the safety of information held; Failure to follow these requirements can hold individuals liable to prosecution and creates an unnessary risk to our people (potentially a threat to life), company operations, and company reputation.

Cyber-attacks are a serious and dynamic threat that is changing how we need to protect our environment before it causes a damaging impact to our organisation. As we move to cloud and mobile driven technologies, the walled-garden approach to security in schools is no longer appropriate. We need to provide a defence-in-depth approach using industry best-practices to secure the entire infrastructure and to control the data within our organisation.

To highlight the significance of a cyber attack and the damage it can do, here are a few recent articles from the UK about targeted attacks to the education sector:

- **"Cyber attack on UK school network affects thousands of students" - The Guardian, Jan 2023.**
  A cyber attack on a UK school network causes disruptions to thousands of students, and highlights the vulnerability of schools to cyber crime.
- **"Cyber attack hits UK exam board, threatens to disrupt exams" - BBC News, Dec 2022.**
  A UK exam board is hit by a cyber attack that threatens to disrupt upcoming exams. The attack highlights the importance of secure IT systems in the education sector.
- **"UK universities face wave of cyber attacks as hackers target research data" - The Telegraph, Nov 2022.**
  UK universities are facing a wave of cyber attacks, with hackers targeting research data and intellectual property. The attacks are part of a global trend of increasing cyber attacks on educational institutions.
- **"UK schools hit by ransomware attack, demand payment to release data" - The Independent, Oct 2022.**
  A UK school is hit by a ransomware attack, and is forced to pay to regain access to its data. The attack highlights the need for schools to implement effective cyber security measures.
- **"Hackers target UK education sector in major cyber attack" - BBC News, Sep 2022.**
  The UK education sector is targeted in a major cyber attack, which aims to steal personal information and research data. The attack highlights the importance of cyber security in the education sector.
- **"UK college forced to shut down after cyber attack" - The Guardian, Aug 2022.**
  A UK college is forced to shut down after a cyber attack affects its IT systems. The attack is part of a wider trend of increasing cyber attacks on educational institutions in the UK.
- **"UK education sector faces surge in cyber attacks, warns NCSC" - Sky News, Jul 2022.**
  The UK education sector is facing a surge in cyber attacks, with hackers targeting personal information and intellectual property. The National Cyber Security Centre warns that educational institutions need to take steps to protect themselves from cyber crime.

These attacks range from highly sophisticated nation-state actors to the more common script kiddies, with the average age of a suspected attacker now just 17. Without adequete controls in place, it is to easy for someone to download and execute pre-built malware that can cause a disruption of services, theft of data, theft of funds, and reputational damage. Unfortunately the majority of 'sophisticated' attacks seen in news articles could have been prevented if the organisation had appropriate security controls in place.

Within this section we outline the security and compliance measures being implemented throughout the trust to mitigate these risks and provide a comprehensive security solution to protect our people and assets.

4.2. Cyber security

So how do we protect ourselves? The first thing to understand is we will never be completely protected as there will always be a risk of attackers that continue to develop sophisticated attacks and breach zero-day vulnerabilities. The key to protecting our organisation is prevention, by making it difficult for someone to breach our systems in the first instance and limiting their ability to traverse the infrastructure using a zero-trust and least privilege approach.

The Department for Education have recently released the "Meeting digital and technology standards in schools and colleges" guidance which provides an extensive list of requirements that schools should meet in order to protect against the vast majority of attacks. In the absence of any previous guidance, this is a welcomed set of documents from the DfE which outline the high-standard of security and technical infrastructure expected of any establishment.

Alongside the DfE guidance, the National Cyber Security Centre have provided a government backed certification called "Cyber Essentials Plus" which contains a strict set of criteria in order to comply with the standard. The Cyber Essentials certification ensures that organisations are implementing core standards to confirm the infrastructure is protected against cyber threats and has an appropriate response and recovery strategy in place. The core objectives covered in the certification are listed below:

1. **Secure Configuration:** Ensuring that devices and software are configured securely, with default passwords changed, unnecessary services disabled, and firewalls configured to block unauthorised access.
2. **Boundary Firewalls and Internet Gateways:** Configuring them to prevent unauthorised access to networks and systems, and to control traffic to and from the internet.
3. **Access Control:** Limiting access to systems and data to authorised users only, with appropriate password policies and two-factor authentication where appropriate.
4. **Malware Protection:** Implementing effective anti-malware software and keeping it up to date to protect against viruses, worms, and other types of malware.
5. **Patch Management:** Applying regular software updates and patches to all devices and systems to ensure that known vulnerabilities are addressed.
6. **Logging and Monitoring:** Configuring systems to log and monitor events, and regularly reviewing logs to identify and respond to potential security incidents.
7. **Security Incident Management:** Having plans and processes in place to detect, respond to, and recover from security incidents, and training staff on these procedures.
8. **Wireless Network Security:** Configuring wireless networks securely, with encryption enabled and default settings changed, to prevent unauthorized access.
9. **Remote Access:** Securing and monitoring any remote access to systems or data, with secure connections and appropriate authentication used.
10. **Backup and Recovery:** Taking regular backups of important data and systems, and testing recovery procedures regularly to ensure that data can be recovered in the event of a disaster or security incident.

Whilst these headings may seem superficial, the level of complexity required to achieve and maintain compliance for each of these categories is momumental when you consider the size of our organisation and the amalgamation of our company, infrastructure, and campuses into a single enterprise environment. With an underinvestment and lack of understanding from our schools of the facilities deployed over the past two decades, there is a significant amount of work and time required to bring all our sites up to an acceptable standard and operating in a fully secure and tightly controlled environment.

With that said, we are committed to achieving the Cyber Essential Plus certification within every school across our trust. The 'plus' variant of the certification goes beyond a tickbox exercise and will involve a full technical audit of our facilities to ensure we have correctly implemented our controls and procedures. This will be a complicated audit to complete, however a vital audit to show our commitment to and execution of securing our entire organisation.

To date, we have deployed an infrastructure within the Microsoft 365 environment that facilitates most technical controls required to protect our organisation. We already satisfy the majority of the standards within the DfE and NCSC guidance and will continue to implement the remaining infrastructure and services required to meet the other standards. We know our current stregths and weaknesses and have been working tirelessly to upgrade, migrate, and amalgamate our infrastructure, services, and processes to continue building a secure and operable environment.

With a rapid expansion of schools joining our trust to double the size of our organisation, we expect a minimum of four years to bring all school up to the expected standard; Primarily due to the rolling programme requirements and impact on budget to replace all legacy devices. Due to the urgency of certain security risks, we plan to migrate every school onto our central infrastructure as soon as possible, replicating our existing model to accelerate the migration process and onboarding of our new schools.

Unfortunately the implementation of this strategic plan will have an implication on school budgets. Throughout the development of our strategic plan we have found ways to make our service efficient and costs effective, however there is an inevitable need for investment from all schools to ensure they meet the required technical and security standards issued by the DfE. With exception to the recent 'Connecting the Classroom' grant, there isn't a specific revenue stream funded by the EFA to support these plans and therefore school leaders will be required to accommodate the additional expenditure allocated to ICT infrastructure and services within their budget.

Overall, our primary approach to security across the trust is to fulfil all requirements set out within the DfE standards for schools and the NCSC CyberEssentials+ certification. This is a comprehensive set of requirements which will be externally audited to ensure our environment remains secure and compliant. Without exposing the technical data in this document, we have already implemented or are currently implementing a comprehensive environment that provides the required technical controls to secure, monitor, respond, and protect our users and infrastructure.

4.3. Cyber incident reponse

We are developing our incident response plan and incident response team inline with industry best practice and guidance issued from the NCSC, ensuring our organisation has an comprehensive strategy to deal with any cyber attack. We will continue to improve the skillset of our response team and develop our documentation and strategy which includes our response plan, recovery plan, playbooks, and incident review process. This process is new to our organisation and will be thoroughly embedded and regularly tested throughout the year to ensure all stakeholders understand their role and responsibilities.

As part of the response process we will follow the guidance issued to report cyber attacks to the appropriate body. This can include the National Cyber Security Centre, Action Fraud, Information Commisioner's Office, Police, DfE Security Enquiries Team, and various other critical contacts and key stakeholders.

Full details of our cyber incident response plan and all technical, physical, and administrative controls can be found in our cyber security policy.

4.4. Compliance

In reviewing the historic infrastructure from our schools, we identified a number of areas whereby our schools have not implemented technologies and practices in accordance with the guidance and legislations within our sector. It is essential that we adapt our practices in line with current guidance to ensure our trust is compliant and operating within the bounds of the law. This includes guidance and legislation from the following documents:

- Meeting digital and technology standards in schools and colleges
    - Broadband internet standards
    - Network switching standards
    - Network cabling standards
    - Wireless network standards
    - Cyber security standards
    - Filtering and monitoring standards
    - Cloud solution standards
    - Servers and storage standards

- Keeping Children Safe in Education
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Data Protection Act 2018 (The UK's implementenation of General Data Protection Regulation)
- NCSC Cyber Essentials+
- SWGfL eSafe360

It is the role of our compliance manager to identify, recommend, and implement changes that ensure our trust is operating within the relevant legislations. All compliance risks will be added to the risk register and DfE technology standards tracker to be reported directly to the CEO, Directors, and other key stakeholders. Any changes made to our strategic plan to accommodate changes in legislation or guidance will be reviewed for ratification by our Board.

A cyber security summary is submitted to all Finance and Personnel subcommittee meetings and our IT Operations Manager also attends all Risk and Audit subcommittee meetings to provide a detailed cyber security and compliance report. This includes the current progress of delivering our cyber and compliance strategy and includes an update of any incidents, alerts, or concerns to address.

5. BUSINESS IMPACT

5.1. Overview

Through the implementation of this strategic plan, we are making significant improvements to the computing environment across the entire trust that will positively impact our students, staff, and wider community. By providing consistent access to a modern, feature-rich facility, we are providing both staff and students with the opportunity to use technology throughout school to provide an engaging and focused educational experience.

Whilst this current strategic plan is targeting the operational requirements of ICT, the long-term aim is to focus on embedding technology into the classroom and working with teachers to implement new tools that can improve the engagement and outcomes of pupils. There are significant benefits to the use of technology in education and this is something to explore further with curriculum leads and staff who want to champion these tools across the trust. The Microsoft Educator Centre has a catalogue of free training and lesson plans, demonstrating new ways of teaching and engaging pupils in the classroom and displaying examples of how technology can be effective.

As of now, there is a clear requirement to overhaul the existing infrastructure and services to provide a facility that is consistent and effortless for our staff. Working in the education sector provides unique challenges throughout each school and by modernising our IT estate we can start to simplify and reduce the workload for our colleagues. If technology becomes a hinderance to our work, it becomes frustrating and adds additional stress. If the technology is trusted to work consistently, then staff will adopt the use technology to assist and improve their day-to-day tasks.

With the additional schools joining our organisation from the acquisition of Horizon MAT, we currently have an estimated two-year technical project ahead to completely migrate all schools onto our modern central facility. At the point whereby our infrastructure is stable and operating effectively, we will identify and engage with key staff across the trust to develop the academic elements of our strategic plan; We will explore methods of embedding technology within the classroom by training our staff and building confidence to use technology effectively.

5.2. Management

Our goal is to provide a managed service that enables schools to focus on education instead of operation. Through a series of structural changes and financial investment, schools will benefit from an organisation wide infrastructure that provides a facility that is consistently operational, secure, and compliant without the overhead and challenges of managing an effective IT strategy.

For the first few years, in line with changes seen across the IT industry, there is a significant investment being made to modernise the existing facilities to ensure they continue to operate effectively as we migrate our resources into the Cloud. Within this investment, we will ring-fence funds as part of a rolling programme that covers the entire IT estate and protects against aging or failing equipment. Once the rolling programme has caught up, over time our operational costs will decrease into a consistent and predictable budget instead of the current volatile purchasing of equipment once it has failed.

We will conduct annual reviews with each school to ensure that the current resources are appropriate to their requirements. We also welcome schools to contact us at any time with any change requests. As part of this review, we will identify the quantity of resources available, the intended purpose, the options available, the upfront costs, and rolling programme long-term affordability. Once everyone is agreement of the requirements, we will merge all purchasing requests across the trust to manage the procurement, implementation, and rotation of our resources going forward.

For schools, this should simplify the management of the entire IT service. By modernising, maintaining, and rotating the infrastructure we drastically reduce any operational risks, and the only requirement from the school is to decide upon the teaching resources required to provide education. All other management duties will be handled by the trust IT team, thus freeing up valuable management time for Headteachers and associated leadership teams.

5.3. Business USP

The core function of our organisation is to provide a rich and stimulating curriculum that strives for the highest academic standards, improves the life chances of the children in our care, and develop our children into well rounded citizens. Throughout the entirety of this plan, we have detailed a significant improvement to the tools and resources available in our classroom that will enable our staff and students to experience an outstanding and world class environment in which to teach and learn.

As a result of modernising our facilities, there are inadvertent benefits that will positively impact our schools. For example:

1. With our schools able to showcase an innovative computing facility, it provides a significant advertisement for any prospective parent or carer looking for the right school for their child. It demonstrates and exemplary use of technology and emphasises a forward-thinking school that can provide their child with an abundance of new opportunities. Whilst it is not the sole reason a parent may choose a particular school; it should go a long way to encourage parents about the positive and opportunistic environment their child is learning in.

2. Our modern facilities could make a positive impact in recruitment and retention of staff across the trust. Whilst it may sound trivial, having a working computing environment can go a long way to reduce stress in the workplace. There are a considerable number of companies who do not invest in technology and provide their employees with either basic or inadequate resources to fulfil their job. When you consider our staff are working continuously on a computer, having an infrastructure that works consistently, is secure, enables innovation, and builds the user's trust is a significant step to keeping them happy and wanting to work for us. The last thing our organisation needs is an employee who is frustrated and unfulfilled as the technology they are working with is either failing, limiting, or does not support their innovation.

3. From a business opportunity perspective, the implementation of an innovative facility and service provides a unique selling point for other schools looking to join our MAT. Having a facility that is efficient, scalable, and provides unique opportunities to collaborate with the other schools in our trust will demonstrate value when it comes to choosing the right MAT to support their needs. The more schools that join our facilities, the more efficient and cost effective our operation becomes, ensuring even higher value in our service.

The points listed above are not an exhaustive list, however, they highlight a few of the additional business benefits of investing in a long-term IT strategy to support the growth and development of our schools.