DDAT

Derby Diocesan Academy Trust

# ICT Strategy

**Approved by Trust Board:14th July 2025**

**Review date: July 2026**

## Contents

## Trust Vision Statement

As a Trust, DDAT aim:

- To promote excellence, equity, and integrity in all that we do, so that our children and young people are well prepared to thrive in an ever-changing world.
- To foster a thriving educational environment where every stakeholder is empowered to excel and flourish.
- To create a network of schools that, grounded in collaboration, innovation, and evidence-based practices, will be beacons of excellence, providing transformative opportunities for all.

This strategy will support the Trust and schools to achieve these aims through:

- Harnessing the expertise of experts in the IT sector
- Protecting our sites through industry leading cyber security practices
- Allowing opportunities for professional development, enriching the IT knowledge of staff
- Supporting school improvement through access to IT systems
- Effectively managing IT resources to help maximise budgets
- Supporting student outcomes through ensuring they have access to IT that will prepare them for the future

## Derby Diocesan Academy Trust Structure

The Trust currently encompasses 34 sites across Derby and Derbyshire. This is made up of 32 primary phase schools (3 infant schools, 2 junior schools and 27 primary schools), 1 secondary school and 1 central team and training hub. This strategy reflects the needs of the range of sites within the Trust and the high levels of autonomy afforded to schools within the Trust, with the ability for school leaders to make decisions based on the needs of their staff, pupils, and families. At the same time, the strategy also recognises the need for the Trust to provide clear directives to schools and users in a time of ever-increasing cyber-threats and reliance on IT systems.

## Rationale

In May 2024, a review of IT systems, solutions and services was commissioned by the Trust Executive team and Trustees, with the aim to inform a future ICT strategy. This strategy draws from these findings, creating a long-term plan that will support DDAT in delivering Trust visions and values, both now and in the future.

The policy has been divided into key areas for action, with a series of short, medium and long term goals. Each section will be informed by industry best practice, alongside the findings of the IT review, ensuring that the strategy is realistic, achievable, and grounded in the needs of schools, staff, pupils, and the wider community. Within each section, the strategy draws from the DfE digital and technology standards for schools and colleges and is also influenced by collaboration with key stakeholders and experts in the field of ICT.

By taking a phased approach, the strategy is set to be achievable by the Trust and its schools, ensuring that sites can manage the complexities of implementing changes to ICT infrastructure and systems, minimising disruptions. The use of phased implementation gives manageable milestones, allowing for the easier allocation of resources, management of risk and tracking of progress.

## Purpose

DDAT have identified that having an ICT strategy across the Trust is not only a technological necessity, but also a valuable tool to streamline processes, reduce the risk of cyber-threats and to help to enrich teaching and learning. The purpose of this strategy is to:

- Ensure all schools within the Trust have secure, stable, and easy to use IT systems that enhance teaching and learning
- Develop a strategy that allows Trust schools to meet DfE digital and technology standards for schools and colleges
- Increase cyber security for all sites and users, strengthening the Trust's cyber security posture, reducing the exposure to cyber security risks and threats
- Provide direction and clear guidelines to support school leaders and teaching practitioners in decision making, providing training where needed
- Cost saving is a significant consideration in the strategy to allow the Trust and schools to make the most efficient use of their budgets
- Supporting DDAT to stay abreast of evolving educational technologies, ensuring they remain competitive and responsive to the dynamic needs of students and educators, both today and into the future
- As the Trust grows, help with onboarding new schools to meet the academies security requirements and to ensure consistency with systems to make it easier and smoother for teaching and learning to at the same standard as the rest of the Trust

The strategy does not seek to influence and impact teaching and learning beyond giving practitioners the IT systems they need to effectively deliver lessons. Through giving practitioners the tools they need, they can use their knowledge of teaching pedagogy to integrate technology into lesson delivery, thus enhancing engagement, collaboration, and positively impacting pupil progress.

## Key Areas

### DfE Standards

The DfE have published guidance under “Meeting Digital and Technology Standards in Schools and Colleges” to help schools and trusts select the right equipment and services to ensure security and reliability of ICT systems. These standards are published on the DfE website and continue to be updated. They can be accessed in full here.

The DFE states these standards should be used as guidelines and will support the Trust in using the right digital infrastructure and technology. In the future, further digital and technology categories will be added to the service. The standards are to be used by everyone involved in the planning and use of technology within schools and colleges, including (but not limited to):

- Senior leadership teams
- IT staff
- Suppliers
- Technical advisers
- Teachers

The DfE Standards currently cover the following areas:

- Broadband Internet standards
- Cloud Solution standards
- Cyber Security standards
- Digital accessibility standards
- Digital leadership and governance standards
- Filtering and monitoring standards
- Laptop, desktop, and tablet standards
- Network cabling standards
- Network switching standards
- Servers and storage standards
- Wireless network standards

Through meeting these standards, the Trust can benefit from making informed decisions about technology leading to safer, more cost-efficient practices and new learning opportunities for pupils.

### Cyber Security

Cyber-attacks and incidents could have significant operational and financial impacts on Trust schools, as well as the PR implications identified within the DDAT IT Review.

The consequences of such attacks include safeguarding issues due to compromised sensitive personal data, negative impacts on pupil outcomes, data breaches, long-term disruptions (including the risk of repeated future incidents and potential school closures), financial losses and reputational damage.

Maintaining robust security and compliance within the Trust is the core focus of this strategy. By leveraging industry security tools, staff training and standards such as NCSC Cyber Essentials, the Trust can maintain a stringent security posture.

### Disaster and Cyber Resilience Planning

It is crucial for all schools within the Trust to have robust Cyber Resilience and Disaster Recovery Plans in place. It is vital to understand the reliance on IT systems and school operations, to plan for the order of recovery should a disaster or cyber attack take place.

Suitable backup methods should be chosen for local and cloud data, along with tested recovery plans that are tested on a regular basis.

### AI in Education

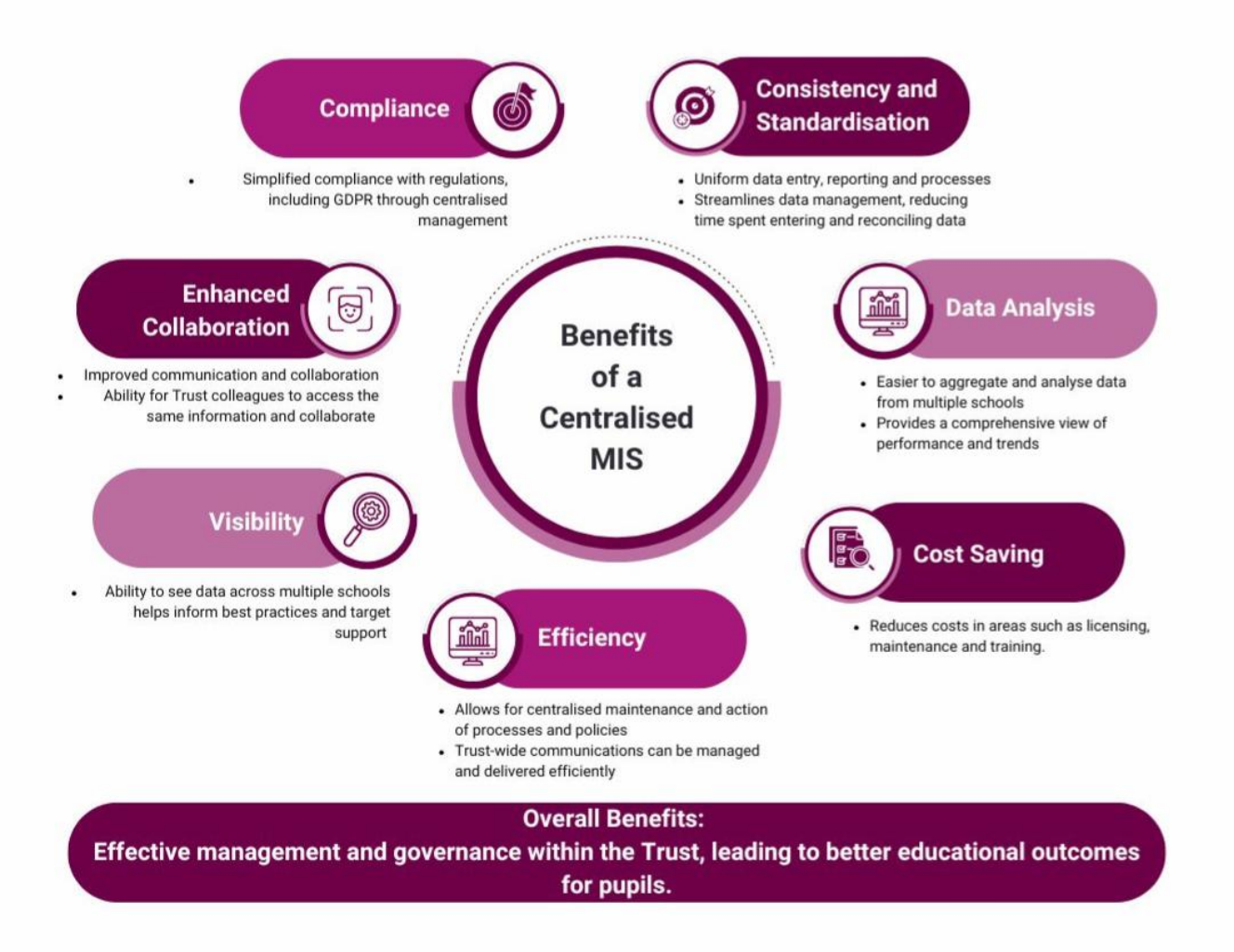
The DfE explains that Generative AI refers to a technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. ChatGPT, CoPilot and Google Gemini are examples of generative AI tools built on large language models.

AI technology is not new, we already use it ubiquitously in everyday life for tasks such as email spam filtering and media recommendation systems in streaming media. Recent advances in technology mean that we can now use tools such as ChatGPT, CoPilot and Google Gemini to produce AI-generated content. The abilities of these tools are increasing rapidly.

The Trust will need to investigate how AI can be helpful and impactful to the schools in the Trust, along with what information should be used on these platforms guidelines and restrictions that should be put in place to protect pupils and staff.

## Management Information System (MIS)

The Trust IT review recommended that the Trust move towards a single MIS system for all schools. Implementing a single Management Information System (MIS) within the Trust offers numerous benefits, outlined in the diagram below:



## KCSIE

The Keeping Children Safe in Education (KCSiE) guidelines set out by the DfE place significant emphasis on online safety and the responsible use of technology in schools. Schools are required to have robust online safety policies that address the 4Cs (Content, Contact, Conduct, and Commerce) integrating these policies into the overall child protection strategy.

Effective filtering and monitoring systems must be implemented to track and manage online activities, helping to identify and mitigate risks related to radicalisation, child exploitation and other online threats. Education and training for staff and students is also key to embed safe online practices, including understanding the risks associated with using information technology and understanding how to report concerns.

The 2024 update to KCSIE includes several additional ICT requirements for schools to ensure online safety and safeguarding. Blocking harmful content alone no longer meets KCSIE requirements. Web filtering logs must now identify the user associated with the web traffic. Sufficient monitoring systems should also be in place to view pupil activity on school devices.

## Cloud Services/Platforms

Trust schools have the autonomy do decide which cloud-based services and platforms they use for lesson delivery and day to day tasks.

Whilst it can be positive for schools to procure the systems that they feel are most suitable for their operations, it does however present several problems for the Trust, including:

- System security may be compromised due to lack of knowledge during the procurement, onboarding and ongoing maintenance of the systems.
- A vast number and variance in systems in use make it difficult for the Trust to support schools with decision making.
- When students or staff move between different Trust schools, common data cannot be easily transferred between platforms.

The role of the Trust will be to identity and audit all cloud platforms in use at all schools, working with practitioners to create a centralised repository of platforms that schools can use to achieve their goals. Through an oversight of all platforms, the Trust will be better placed to ensure that systems have the correct security configurations and are adequately maintained.

## Microsoft 365

Microsoft 365 provides a suite of productivity tools and cloud-based services. Not only does this include applications such as Word, Excel, PowerPoint, and Outlook, it also includes collaboration tools such as Microsoft Teams, SharePoint, and OneDrive. These services provide cloud storage that can be accessed from a web browser on any device that is internet connected. The email mailboxes for all Trust sites are stored within the Microsoft platform.

As more data moves to the cloud in line with DfE guidance, Microsoft 365 provides a cost-effective and scalable service with robust security features, if configured and maintained to a high standard.

With the Trust already consisting of a sizeable number of schools and growing, there is a need to explore the most suitable way to structure the Trust Microsoft 365 tenants. By establishing the benefits and drawbacks of each approach we can create a scalable model that aligns with the vision of the Trust.

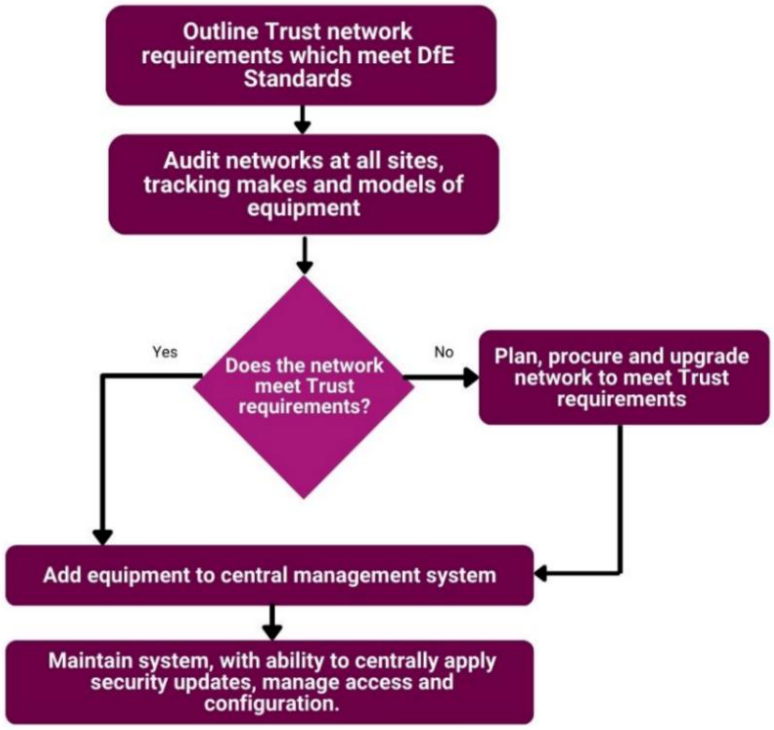
## Networking

The DDAT IT review highlighted a vast variety of networking equipment and standards in place across the schools within the Trust. Many schools have benefitted from the DfE “Connect the Classroom” initiative, but there is still a large number of schools that would benefit from upgrading their networking infrastructure.

The strategy will outline the steps needed to bring all Trust schools to the same level, whilst adhering to the DfE standards.

The DfE standards states that any new networking equipment should be cloud managed. The Trust would benefit from choosing a single vendor and management platform for any future hardware acquisitions, to give a central overview and configuration of all sites within the Trust. Central management also provides a means of monitoring performance, uptime, and the fast deployment of security updates to equipment. Such a platform enables fast and consistent configuration changes, an example of this could be the deployment of a Wi-Fi network for the DDAT central team to access at all schools.

**Networking Refresh Process Flow:**




## Printing

Currently, schools within the Trust procure and manage their own photocopier contracts.  The schools are using a range of companies and manufacturers, leading to fragmented and potentially costly arrangements.

To optimise operational efficiency and cost-effectiveness, it would be beneficial for the Trust to centralise the printing contracts all schools. By consolidating the contracts, the Trust can leverage bulk purchasing to secure more favourable pricing, resulting in significant cost savings.

Centralising a system that utilises cloud printing will streamline operations, allowing staff and students to print documents seamlessly across all locations within the trust, regardless of their physical location.

### Devices

As established within the Trust IT review, schools within the Trust use various devices to enhance learning, develop technological literacy, and improve collaboration. Users of devices fall into three main categories: Windows devices, Chromebooks, and tablets.

Device procurement decisions are limited to the knowledge the schools have access to, whether that be internal staff or a reliance on third party IT staff. This often leads to the wrong devices being procured for their intended purpose, either by purchasing sub-standard hardware or under/overpowered devices. As result there are financial implications for the Trust and potential disruptions to school operations if devices are unavailable for use.

This strategy will outline the need for the Trust to assess the purpose of devices used within schools to produce recommended device specifications according to their intended purpose. The medium term plan will also outline the potential benefits for central hardware procurement.

Device lifecycles will need consideration, as devices only receive necessary security updates for a specific amount of time. The end of these updates and time of ownership needs to coincide as part of a regular rolling replacement strategy. The creation of a central asset register will support decisions, helping to determine the devices currently in use and device refresh budget requirements.

### Device Management

The Trust IT Audit has highlighted that schools are currently maintaining devices through various methods such as on site servers, mobile device management (MDM) or no device management. Device management is a key consideration within this strategy to ensure software and security updates can be effectively deployed and maintained.

Inadequate device management can disrupt teaching and learning and could lead to safeguarding implications. Within the phases of the strategy will be the implementation of a Trust wide MDM and RMM (Remote Management and Monitoring) system.

A Trust wide MDM and RMM system would ensure that key security is implemented and maintained. The systems would be setup as a central system that would maintain devices on behalf of schools. Having central systems would guarantee security is the same for all schools instead of relying on maintaining multiple systems. A single change can be implemented that would affect all schools and devices, not one change multiple times. With the MDM Microsoft Intune, licences are already included to already access the platform and there is no further costs or time wasted to identify and test other platforms.

### Classroom Hardware

Each school currently holds their own asset register and hardware replacement strategy, but these audits and strategies may not be the most effective for the school's needs, mainly due to the resources and expertise that can be allocated to produce a potentially inferior strategy.

Auditing the classroom equipment across the Trust and creating a classroom hardware standard will ensure that adequate hardware is purchased and that all schools classrooms are functioning to the same level. A clean asset register alongside a device replacement strategy will help to improve reliability, security and an average lifespan.

## Phones

Currently each school procures and manages their own phone system. This has an impact on cost and the systems may not be the most effective for the needs of the school. Schools are not likely to have the correct resources and expertise required for procuring and maintaining the systems, potentially leading to misconfigured, unsecure and inferior systems.

The benefits of a centralised phone system include:

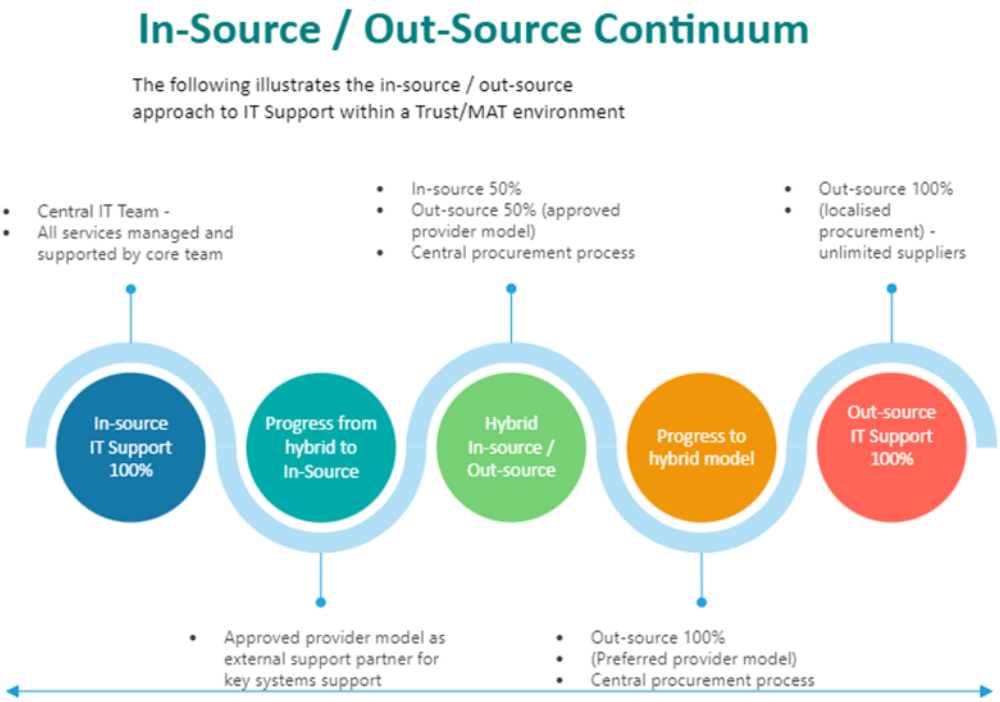

The strategy will outline the steps needed to design and implement a centralised phone system, to be centrally procured by DDAT with an optional buy-in to be offered to Trust schools. The latter stage of the strategy is for all DDAT sites to be enrolled onto the central phone system.

## ICT Support

At present, each DDAT site procures and maintains individual ICT support contracts. Each school evaluates their needs and procures a company of their choice to support their school. ICT support plays a crucial role in helping the Trust schools to both function on a day-to-day basis, but also on an ongoing basis when looking at implementing the IT Strategy, especially security requirements.

To help to meet the IT strategy and implement key initiatives, an important first step will be outlining a set of standards that each ICT support provider must meet. The Trust will then need to audit each school's ICT contract to ascertain whether they are meeting the necessary standards. The Trust should put in place regular review meetings with each ICT support provider to ensure key milestones for implementing the IT strategy are met.

The Trust IT review report raised an important consideration to improve the IT support received by schools. The Trust will explore how future IT support is delivered and will outline the key phases to move towards.



## Sustainability

To ensure sustainability with Trusts ICT hardware we can adopt several effective strategies. We can prioritise energy-efficient devices, such as those with ENERGY STAR certification to help reduce power consumption and lower utility bills. Investigating remanufactured or refurbished equipment supports the circular economy and can offer a cost effective solution. Implementing cloud based solutions minimises the need for on-site hardware, thereby reducing e-waste and energy consumption.

Using a central asset register will help track and manage all ICT hardware, ensuring efficient use and identifying opportunities for repurposing and donating devices. Establishing device recycling programmes ensures proper disposal or repurposing of old devices, while implementing secure wiping protocols guarantees data protection before recycling. Partnering with reputable recycling companies will ensure environmentally responsible disposal of electronic waste.

Educating staff on best practices extends the lifespan of technology and reduces repair costs. Additionally, exploring leasing or buy-back schemes can provide financial benefits and positively impact teaching and learning.

Investigating and implementing the printing solution PaperCut could help with printing sustainability.  Papercut includes features that can reduce waste and cut costs by encouraging responsible printing practices such as double-sided and grayscale printing. Additionally, it provides full visibility into print usage, helping to manage resources more effectively.

We can significantly reduce our environmental footprint and contribute to a more sustainable future.

## Actions

### Short Term – Within 1 Year

#### DfE Standards

The Trust must ensure that all new contracts comply with the Department for Education (DfE) requirements. If it is not feasible to meet these requirements directly, the contracts must be reviewed and approved by the Trust before renewal.

The Trust will conduct an annual review of the current Department for Education (DfE) standards to identify any changes or updates in the standards, allowing the Trust to adjust its plans and practices accordingly.

#### Cyber Security

Ensure MFA is enforced for all staff on all systems containing sensitive information. Multi-Factor Authentication (MFA) enhances security by requiring users to provide two or more verification factors to access resources such as applications or online accounts. This additional layer of security significantly reduces the risk of unauthorised access. This is crucial for DDAT as schools are frequently targeted by phishing attacks. MFA helps protect against these attacks by ensuring that even if a user's password is compromised, an attacker would still need the second factor to gain access. This added security measure is vital in safeguarding sensitive information and maintaining the integrity DDATs Schools digital resources.

For all Trust Microsoft 365 tenancies, Multi-Factor Authentication (MFA) will be enforced for all staff accounts. This not only strengthens the overall security but also ensures compliance with the DfE requirements. This needs to be confirmed that is has been actioned by the ICT support provider for each school.

#### National Cyber Security Centre Recommendations

The National Cyber Security Centre (NCSC) is a UK government entity that provides guidance and support to protect against cyber threats. It aims to make the UK the safest place to live and work online by offering expert advice, managing cyber incidents, and collaborating with international partners.

The Trust will ensure that each site within the Trust is set up on the MyNCSC portal, with all school domains added to the Trust's view on the portal. This will facilitate the National Cyber Security Centre (NCSC) recommendations implemented at each school, enhancing overall security. The portal will provide a summary of information for all schools, highlighting areas where improvements are required. It will be particularly useful for managing websites and email security, ensuring that these critical services are consistently monitored and protected. By using the MyNCSC portal, the Trust can benefit from streamlined security management, improved compliance with NCSC guidelines, and a more robust defence against cyber threats. This system will have a significant positive impact on the Trust's ability to safeguard its digital infrastructure and maintain a secure environment for all its schools.

Baseline Security Standards Register

Currently, DDAT schools operate on separate systems, each with its own computer networks and Microsoft 365 tenancies. To enhance cybersecurity across all schools, the Trust needs a unified approach to ensure maximum protection against cyber threats.

To achieve this, the Trust will establish a baseline set of security standards that must be enforced at each school. The baseline security will be created based on NCSC Cyber Essentials. This will ensure the Trust is protected at the very least from common cyber threats and that data is safe from cyber-attacks. NCSC Cyber Essentials is a Government backed certification scheme.

The baseline security standards will help safeguard users and data from the increasing risks of cyber threats, ensuring that every school within the Trust meets the necessary security requirements and will guarantee a high level of security across all Trust sites.

This should include the following areas:

- Microsoft 365
- Google Workspace
- Servers and Domains
- Client Devices
- Mobile Device Management
- Networking

The Trust will create a required baseline security standards document which will need to be communicated to each school. Each school will need to confirm that each point has been configured and implemented and provide any information regarding implementation or any issues incurred. For any areas that are not already implemented, a plan must be put in place to complete implementation. This will then be followed up by the Trust to ensure compliance and consistency.

All areas of security must be kept up to date on a centrally held security register to ensure there is a quick and straightforward way to track what security settings are in place at each school.

Please see Annex 1 – for an example of the baseline security standards for Microsoft 365. This will need expanding on for the other areas.

The baseline security standards will need annual revision due to the ever-evolving nature of ICT, any updates to the standards will need to enforce for each school, and the security register updated.

Annual Trust Security Audits

The Trust will conduct annual audits to proactively address emerging threats and adjust security as necessary. Any identified issues must be implemented across all schools. The security register will be updated to reflect the completion of these checks.

## Training

All staff need to undergo regular cyber security training to protect sensitive information and ensure the safety of data and school systems. With increasing reliance on digital tools and online platforms, schools are prime targets for cyber-attacks, which can lead to data breaches, financial loss, and disruption of educational activities.

Training helps staff recognise and respond to potential threats, implement best practices for data protection, and maintain a secure digital environment. This proactive approach enhances the overall cyber resilience of the trust.

### *Cyber Security Training*

The Trust will ensure cyber security training will be completed by all staff in all roles with email accounts, including Local Academy Committee Members, Trustees and midday supervisors. This is a key part of meeting the terms of the Risk Protection Arrangement (RPA) cover. The training will utilise the NCSC's "Staying Safe Online: Top Tips for Staff" e-learning package, which has been identified as a quick and effective training tool. The training we will look at how and why cyber-attacks happen. They will also give some tips to ensure staff are practising good cyber hygiene in both the workplace and at home. They will look at the types of people that might be a risk to the workplace from a cyber security perspective. They will also look at the practical steps to take to protect themselves and school from cyber-attacks. The training will be tracked for all staff.

### *Microsoft Attack Simulation*

The Trust will ensure Microsoft's attack simulation training will be completed by all staff with email accounts randomly throughout the year. Microsoft's attack simulation training is part of Microsoft Defender for Microsoft 365. It will allow realistic cyberattack scenarios to test and improve our security. The simulations will help identify any vulnerable users and train them to recognise and respond to threats such as phishing, malware, and other social engineering techniques. Using this training we will be able to provide detailed reporting to help understand security weaknesses and improve our defences against threats. This proactive approach enhances overall cyber resilience by preparing employees to handle real-world cyber threats effectively.

## Backup

To meet the Risk Protection Arrangement (RPA) and Department for Education (DfE) standards for backups, all schools will follow these guidelines:

1. **Three Backup Copies**: Maintain at least three backup copies of important data.
2. **Separate Devices**: Store these backups on at least two separate devices.
3. **Off-Site Storage**: Ensure that at least one of these backups is stored off-site.

4. **Offline Backup**: At least one backup should be held entirely offline and only connected to your systems when necessary for restoration.

### Audit Backups

As per the DfE guidance, the Trust will audit the backup systems and processes at each school will need to identify the following:

- What data is currently being backed up
- How often data is backed up
- How old the data is and how it is being backed up - this will include data stored on all cloud services, this information will be stored in our information asset register
- What information is not being backed up
- How often the test data that has been restored to check the backups are successful
- How long a restoration will take and when the last test restoration was completed
- How many copies are being kept and where they are located
- How your backups may be affected in the event of an incident or attack

### Centrally Procure Backups

The Trust will focus on procuring a centralised backup solution, specifically for Microsoft 365, that complies with all RPA and DfE requirements. For schools with data stored locally on servers located within the schools, the trust will procure an offsite backup solution.

Once this backup solution is chosen, schools within the Trust will have the option to purchase directly from DDAT. Alternatively, schools can choose to implement their own backup solutions, provided these meet the specifications set by the Trust. It is essential that each school documents their chosen backup solution and ensures it is recorded in the central security register. This process will help maintain a high standard of data security and ensure compliance across the Trust.

## Management Information System (MIS)

In the recent IT review, it was recommended that the Trust transition to a single Management Information System (MIS) for all schools. This move is expected to significantly enhance the Trust's ability to access and manage a standardised data set across all schools. By consolidating the MIS, the Trust can ensure more consistent data handling, improve efficiency in data management, and facilitate better decision-making processes based on uniform and reliable information from all schools.

When a MIS is implemented, it is crucial for staff to undergo extensive training and have access to comprehensive documentation. This ensures that they can work efficiently and effectively with the new system. Proper training helps employees understand the functionalities and benefits of the MIS, while thorough documentation serves as a valuable reference for troubleshooting and optimising their use of the system. Together, these elements are essential for maximising the productivity and success of the MIS implementation.

The Trust will initiate the procurement process for a new MIS that will be standardised across the entire Trust. This involves identifying and selecting a suitable MIS that meets the needs of all schools. A detailed plan for the implementation of this system will be developed to ensure a smooth transition. This plan will outline the steps required for installation, staff training, and integration with existing systems, while aiming to enhance data consistency and operational efficiency across the Trust.

### KCSiE

#### Audit

An audit will be carried out on the systems currently in place at all schools within the Trust to ensure KCSIE is being met. If this audit reveals any areas where these requirements are not met in full then they need to be remedied as soon as possible.

The Trust will need to investigate centrally procuring a monitoring system that can be deployed to all schools. The system will alert designated school staff to students becoming vulnerable based on their digital behaviours that can give the central team an overview and notifications of any safeguarding concerns.

### Microsoft 365

#### Tenancy Type Investigation

The Trust will need to investigate and compare the type of tenancy structure to be used.

- Single Microsoft tenancy – Single tenancy that stores all users' emails, data and devices etc
- Set of Hub Tenancies – Similar to a single tenancy but instead have something like 4 setups for the different of areas of school's locations
- Individual School Tenancies - Each school and DDAT have their own tenancy, but they have shared access to easily share data

This investigation should look to balance the following areas before a decision is made:

- Ease of Management of multiple tenancies
- Ensuring Security parity across the trust
- Ease of data sharing for users
- Standardisation of email addresses, Teams locations and data storage

Once the investigation has been completed, a proposal will be put to the Trust to make the decision of which model is the best to progress with.

#### Setup

Once a decision has been made, the setup of the tenancy/tenancies will be implemented. Moving towards the medium term strategy considerations will need to be made for the timeline, project planning and implementation for all school sites.

### Central Team Data

The central team's data will be migrated from Google Drive to Microsoft Teams/SharePoint. Microsoft Teams integrates seamlessly with other Microsoft 365 apps, facilitating a more cohesive workflow by allowing easy access and editing of documents directly within Teams. Microsoft's system is more user-friendly for administrators to maintain data and sharing as Google Drive is designed more for individual users sharing data rather than a shared data platform. At present DDAT has security measures in place on the Microsoft 365 tenancy, requiring minimal extra configuration.

## Networking

### Audit

To start moving towards a standardised networking estate a full audit needs to be carried out that highlights areas where the networking systems do not meet the DfE Standards. This audit will also need to include the makes/models of equipment so that a plan can be made to replace and improve the systems in place.

The following will need to be audited:

- Networking
    - Switches Make and Models
    - Hardware and Cabling Age
    - Cabling specification – Cat 5e, Cat 6 etc
    - Network Layout – Switch, Servers Internet etc
    - Network Speed test
    - Network Configuration – VLANs etc
- Wireless
    - Hardware Make and Models
    - Hardware Age
    - Wireless Standards/Compatibility. WiFi 6 should be the minimum, as set in the DfE Standards
    - Configuration
- Internet
    - Internet providers
    - Internet expected speed
    - Onsite speed test

### Recommended Specification

The Trust will ensure a recommended specification is in place to be shared with all schools so that future purchases can be aligned across the trust. This will help maintain a high standard of security and ensure compliance across the Trust.

Please see Annex 3 for the Networking Specification.

### Wireless Improvements

All schools will need to set up and configure a new guest Wi-Fi network, with details provided by the Trust. Each guest Wi-Fi will have Access Control Lists (ACLs) to

prevent access to the main school network, ensuring the security of existing school devices and servers. This setup will allow the central team and any roaming staff members visiting other schools to have instant access to any trust school's internet. This is documented in the BYOD policy under the Guest Wi-fi section.

### Printing

Current Contracts
An internal audit will need to take place of all schools with what current providers and what they are providing and when the contracts are expiring. This will help feed into planning a rollout process of a centralised printing system across all schools. All schools will only be allowed to renew up to 1 year with the intention of rolling out the new solution Trust wide almost simultaneously.

Investigate Solution
An investigation will take place into a central provider who can eventually support all schools in the trust. The new provider and system will ideally be cloud based with the ideal solution of all trust staff and students being able to print to the same printer no matter what school they are located and releasing the print at the nearest local printer.

### Devices

Ensure devices are no longer running Windows 10
Microsoft have announced that Windows 10 support will end on the 14th October 2025. After this date Microsoft will no longer issue security patches and updates. The Trust needs to ensure that there are no devices within the trust that are still running Windows 10 by this date to guarantee that the devices are not vulnerable to security risks.

All devices will need to be running Windows 11 (or later) by this date. Some devices will have the possibility to be upgraded, however windows 11 has more strict hardware requirements so there will be devices that cannot be upgraded and will need to be replaced.

To achieve this by October 2025, the Trust will need to audit all devices within the Trust. A plan must be put in place to upgrade/replace the devices before the deadline.

Define minimum standard for new devices

Implementing minimum standards for IT devices in schools is essential for ensuring security, compatibility, and cost efficiency. It helps protect student data, streamlines procurement, and reduces maintenance costs. Standardised devices enhance productivity by providing a consistent user experience and simplifying IT support. Adhering to industry regulations ensures compliance and best practices, creating a secure and efficient learning environment. The minimum standard for devices must meet or exceed the published standards from the DfE. This section overlaps with the DfE standards.

This should include the following areas as a minimum:

- Laptops
- Desktops
- Tablets
- Networking equipment including wireless

We have chosen to use the DFE's Laptop, desktop and tablet standards to create our baseline.

Meeting digital and technology standards in schools and colleges - Laptop, desktop and tablet standards - Guidance - GOV.UK

Following the baseline being created, all schools will be informed of the new procurement baseline and expectation.

Investigate Central Asset Register

A central asset register could improve the efficiency of asset management, financial accountability, and risk mitigation. The register could help to track and maintain assets, ensuring they are used effectively across the Trust. This centralised system needs to support accurate financial reporting, strategic planning, and proactive maintenance, enhancing operational efficiency and reducing costs. Schools will be asked to share up to date asset lists, which will be imported to create a centralised register.

### Device Management

Investigate and Configure Central MDM Intune

Once configured, this system could be offered out to schools without an existing MDM or at the time of renewal for their current MDM.

Investigate RMM (Remote Monitoring and Management) Tool

Trust to investigate an RMM Tool to help to remotely and proactively monitor endpoints and network infrastructure. Information is gathered regarding each connected device to provide detailed insight and configuration options.

### Central Team Setup

Once the MDM and RMM tools have been finalised and setup, all Central Teams devices will be enrolled.  Any new devices procured will be automatically joined to the MDM where the RMM tool will always be deployed.

## Classroom Hardware

### Audit

Audit classroom hardware across the Trust.

### Create Classroom Hardware Standard

The Trust will create a classroom hardware standard with the eventual aim of bringing all school classrooms to the same level.

## Phones

### Investigate Cloud Phone System

As BT is closing the Public Switched Telephone Network (PSTN) by 31 January 2027, the Trust will investigate a new IP cloud hosted phone system as a traditional phone system will no longer be an option.

The investigation will need to be linked to the internet connectivity and filtering audit to ensure each school has the required connectivity to support a cloud hosted phone system.

### Provide as Option for School Implementation

Once the phone system has been finalised and setup, the Trust can offer as an optional service to all schools.  This will aim to save the schools money and management time but also a quick and seamless way for schools to communicate.

## ICT Support

### Audit

A full audit of all schools ICT support contracts needs to be actioned. The audit will need to include what is provided by each of the providers. Once completed the audit needs to be compared to the Trust’s minimum requirements.

### New Contracts

When school contracts conclude, they must be reviewed by the Trust to ensure compliance with the Trust's requirements. Additionally, all new contracts will incorporate regular review meetings with the Trust stakeholders.

## AI in Education

As AI is an area that is developing quickly, a review needs to be carried out to ensure that the AI Policy is up to date with the current use cases for AI. The DfE have a policy paper that can be used to facilitate: Generative artificial intelligence (AI) in education - GOV.UK

## Sustainability

### Central Asset Register Audit

The information from the central asset register device audit will be used to identify assets that can be repurposed, donated or recycled.

### Device lifecycle management

Investigate extending the life of devices through maintenance and repairs if they meet security standards and are in a reasonable condition.

Any devices that cannot be repaired can be donated to local community organisations, charities, schools in need or recycled.

### Repurpose and Donate

Devices that can be repurposed will be reused for non-intensive tasks within other DDAT Schools if they meet security standards and are in a reasonable condition.

Any devices that cannot be repurposed can be donated to local community organisations, charities, schools in need or recycled.

### Implement Data Security Measures

Any devices that are to be donated or recycled will need to make sure that all data is securely wiped.

### Partner with Certified E-Waste Recyclers

Investigate and work with reputable e-waste recycling companies that adhere to environmental and ethical standards but also maintain data privacy and comply with GDPR regulations.

### Sustainable Procurement

When procuring devices, choose suppliers with strong environmental credentials. Investigate refurbished or modular devices where possible.

### Energy-efficient hardware

When procuring devices, prioritise low-energy devices (e.g. Energy Star-rated).

### Power management

Implement automatic sleep/shutdown policies for equipment such as computers, monitors, printers, interactive boards etc.

### Cloud and Virtualisation

Move to cloud-based systems to reduce reliance on local servers while also reducing e-waste and energy consumption.  The use of virtual machines could consolidate workloads and reduce hardware needs across the trust.

### Data and Monitoring

Investigate tracking and visualising the all DDAT buildings energy use, carbon footprint, and progress toward sustainability goals.

## Medium Term – 3 Years

### Backup

Central Backup Services
Schools to migrate to central backup services as current contract contracts end in order to achieve the best value for the Trust.

### Devices

Central Asset Register
Implement central asset register across all Trust schools. Specific staff at each school will have delegated access view only their own school data. The central asset register will be used to help create a regular replacement program for all hardware across all Trust schools.

Central Hardware Procurement
The Trust will have the capability to procure and store hardware in bulk for all schools. The Trust can achieve cost savings by purchasing hardware in larger quantities than individual schools typically can.

Investigate One to One Devices for Students
The Trust will investigate the impact and feasibility of deploying devices to students on a one-to-one basis. The investigation will include the following but will also need expanding on:

- Lifetime cost of device
    - Cost to purchase
    - Warranty and expected repair costs
    - Lifetime of device
    - Cost of device management and licensing
- Parental contributions
- Potential savings on devices needed in school ie laptop trolleys/iPads.
- Potential for saving on paper and other printed resources
- Type of device (Chromebook/Laptop/Tablet)
- Ongoing affordability and sustainability

### Data Protection

The Trust will investigate all cloud hosted platforms used by all schools. It will be investigated which platforms are required and which are not. A central list of approved online services that meet the security requirements of trust will be created and schools will be able to contact the Trust for a system which will help meet there needs, for example a school may need a system that provides online maths resources.

For any new systems a school has been recommended or enquired about, schools will always need to contact the Trust for approval. This will include all free and paid for systems. The Trust will be able to assess the system and implement a centralised GDPR Data Protection Impact Assessment (DPIA) that encompasses all

DDAT schools. All new systems will need to support SSO (Single Sign On) for security using Microsoft 365. This will ensure that security already implemented on Microsoft 365 will automatically be implemented.

### Management Information System (MIS)

With a central MIS system in place the Trust will ensure this is implemented across all schools. Training will be organised and implemented at all schools. Data will need to be transferred to the central MIS system.

### KCSIE

#### Single Safeguarding System

A single safeguarding system will be investigated and procured to meet the needs of DDAT and all schools. A specification will be created and used to choose the most suitable platform to provide a secure system for recording and managing all types of safeguarding concerns. The system will need to support SSO with Microsoft 365 to adhere to the trusts security.

#### Filtering and Monitoring

The Trust will investigate centrally procuring internet filtering and monitoring for all schools. The system will need to meet the DfE requirements for both KCSIE and the Meeting Digital Standards. The procured system will be implemented to all schools when existing internet and filtering contracts expire. If a school chooses not to use the central system, the school must use a known product by the Trust and be configured to alert the central team to safeguarding alerts and concerns

### Cloud Services/Platform

All new cloud services/platforms must support Single Sign On with Microsoft 365 to ensure security and ease of use for pupils and staff.

### Microsoft 365

#### Configuration and Implementation

Based on the investigation of implementing a single tenancy or hub tenancies, schools will continue with the migration to the chosen model.

### Printing

The new printing solution will be fully implemented at the Trust and will be live for the central team. As schools printing contracts end schools will not be able to renew, extend or procure any new contracts, instead they will have the central system implemented.

### Networking

#### Utilising Current Equipment to support other schools

Spare equipment will be reallocated from site to site to improve the overall estate. Several schools have benefited from the government scheme CTC therefore spare equipment can be utilised where improvements can be implemented raising the standards while offering cost savings. Any unusable equipment will be recycled.

### Device Management

MDM Systems
All schools will be required to have an MDM solution in place and all devices will be enrolled into the solution.

### Classroom Hardware

Rolling replacement program
A rolling replacement program will be implemented by the Trust. The replacement program will ensure that all hardware is replaced in a regular time frame leading to devices being retired before becoming legacy devices (devices not supported by manufacturer or not receiving security updates) but also a budget can be planned.

For example, a computer or laptop could be replaced every 5 years. If the trust had 1000 computers or laptops then 200 would need to be replaced each year.

### Phones

Centralised phone system
Migrate schools to central phone system as contracts end.

### ICT Support

Procurement Process
The Trust will investigate up to four ICT Support providers that the trust schools can choose to use. The Trust will ensure that the four recommended providers offer adequate support that meet's Trust requirements.

ICT Support standards
Set standards that ICT support contracts must meet.

### Sustainability

Adopt Green ICT Practices
Investigate the use of energy efficient hardware and smart technologies to reduce energy consumption across the Trust. Implementation of smart lighting and energy monitoring systems will help optimise energy management and use.

Investigate Circular Economy Sustainable ICT
Sustainable IT is based on the circular economy model. This is a positive move away from the old linear product creation style of 'take-make-dispose', to a more sustainable 'make-use-recycle' route, making the most of our planet's limited resources.

When seeking to purchase IT hardware such as laptops or tablets sustainably, there are several options available. The two primary options are buying remanufactured or refurbished equipment and participating in leasing or buy-back schemes.

Investigate the use of refurbished or remanufactured ICT equipment, as well as leasing or buy-back schemes, to determine their cost-effectiveness and impact on teaching and learning.

DDAT could also support initiatives that focus on the reuse and recycling of electronic components across the Trust.

## Long Term – 5 Years

### Devices

Rollout Devices for Students
Subject to the conclusion of the investigation into the potential one to one roll out of devices to students, start the planning and procurement process.

### Networking

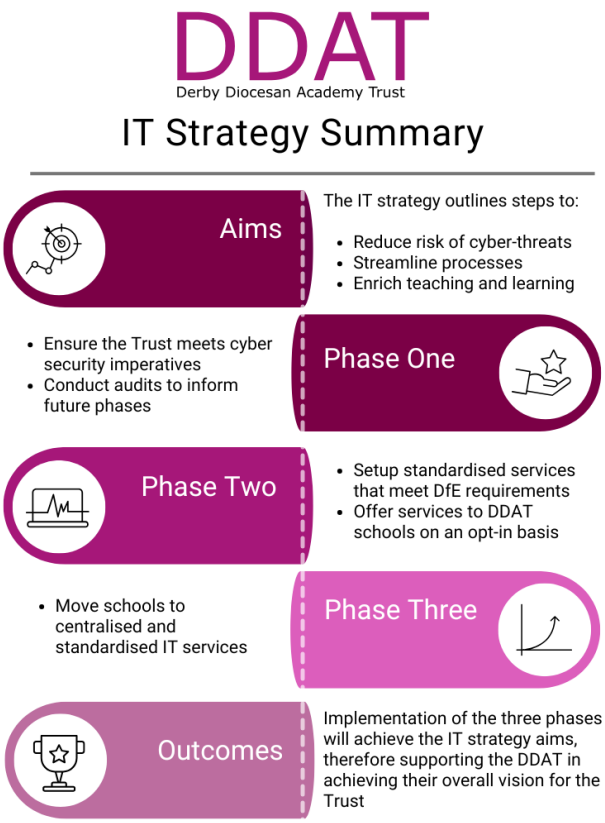
Central Management
All replacement hardware will be centrally managed by the Trust's preferred Network infrastructure solution.

## Summary

Having outlined the key priority areas for the Trust, this document provides a concise roadmap for meeting the aims of streamlining processes, reducing the risk of cyber-threats and enriching teaching and learning. The strategy outlines a three-phase process, grounded in the following stages:

- Phase One – Meet cyber security imperatives and conduct necessary audits to inform future phases
- Phase Two – Setup standardised services meeting DfE requirements and offer these to schools
- Phase Three – Move towards centralised and standardised IT services

The short, medium and long term goals work towards this three-phased approach.




The phases within this IT strategy are designed to support the Trust in their overall aims of ensuring that children and young people are well prepared to thrive in an ever-changing world, ensuring that Trust schools benefit from innovation and evidence-based practices.

| Item | Short Term - Within 1 Year | Medium Term - 3 Years | Long Term - 5 Years |
|---|---|---|---|
| **Cyber Security** | Ensure NCSC recommendations are configured at each site, with all school domains added to trust view on MyNCSC portal | Have set Security settings on Office 365 Tenancies that | |
| | Ensure MFA enforced for all staff (meeting DfE requirements) | | |
| | Create set of Security standards that are required at each site (particularly Office 365) | | |
| | Audit by ICT Manager - Annually | | |
| **Devices** | Windows 10 - Upgrade/Replace before October 2025 | Annual device procurement program on behalf of schools that elect in - to reduce costs | Have rolling replacement program up and running, ensuring that unsupported devices are removed from the system. |
| | Set minimum standard for new devices for Admin/Teachers/TA's/Students | Implement Central Asset Register across all sites with delegated access for each school | Start procuring devices centrally |
| | Investigate Central Asset Register | Use Asset register to create rolling replacement program across trust | |

| Item | Short Term - Within 1 Year | Medium Term - 3 Years | Long Term - 5 Years |
|---|---|---|---|
| **KCSIE** | Audit all schools to ensure KCSIE is being met | Move to single Safeguarding System - Myconcern/cpoms etc<br>Have set product for filtering/monitoring which can be procured by the schools or centrally but must be a certain known product and configured to alert central team to safeguarding alerts | Centrally Procure internet/filtering for all sites. Ensure this system meets the DfE requirements for both KCSIE and the Meeting Digital Standards |
| **MIS** | Audit MIS contracts<br>Start Procurement of new MIS that will be standardised across trust | Ensure all school on central MIS | |
| **AI in Education** | Strategy should include policy for AI in education - or at least link to one. | | |
| **DfE Standards** | Ensure new contract meet DfE requirements or are checked with trust central team before renewing if not for any reason. Includes:<br>Internet Connection/Filtering<br>Cloud Solutions<br>Cyber Security Standards | | |
| **Item** | Short Term - Within 1 Year | Medium Term - 3 Years | Long Term - 5 Years |
| **DfE Standards** | Digital Accessibility | | |

| | | | |
|---|---|---|---|
| | Full list here: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges | | |
| **Networking** | Configure Guest wifi at each school with details provided to Central team | Investigate and look to set a make/model of networking/wireless so that new systems will match across trust | Move towards centrally managed networking where possible |
| | Audit current WiFi Systems and standards across schools | Re-allocate spare equipment from site to site to improve overall estate for example some sites will have benefited from CTC, they may now have spare equipment that is better and newer that isnt being used than the equipment at other sites - cost savings | |
| **Phones** | Set up central phone system that schools can buy in to | As contracts end, move schools over to the central system | |

| **Item** | Short Term - Within 1 Year | Medium Term - 3 Years | Long Term - 5 Years |
|---|---|---|---|
| **Office 365** | Set up central Tenancy that schools can elect to use (@school.ddat.org.uk) | | |
| | Migrate central team data from Google to MS Teams/SharePoint | | |

| | | | |
|---|---|---|---|
| | Investigate single tenancy vs Hub Tenancies - Look at central management of multiple tenancies | | |
| **ICT Support** | Audit ICT Support contract - info held by central team | Decide on 3-4 ICT Support provides - schools can choose from them only at contract renewal | |
| | Set up central list of contracts for ICT services etc with RAG rating to properly identify missing requirements rather than relying on feedback from schools | Alternatively, ensure that each support provider has regular review meetings with the trust IT Manager provided as part of the contracts | |
| **Data Protection** | Central list of where data is held | Approval from central team/gdpr team for new online services - free or paid | |
| | | New systems look to have Single Sign on/Sign on with Office 365 etc | |

| **Item** | Short Term - Within 1 Year | Medium Term - 3 Years | Long Term - 5 Years |
|---|---|---|---|
| **Backup** | Audit Backups of schools/Office 365 - Ensure all sites meet DfE Standards and RPA requirements | As contracts end, move towards central backup option | |
| | Centrally Procure Office 365 Backup - Allow schools to buy in | | |
| **Device Management** | Set up central Management System (intune already in place) | Require all schools to have an MDM solution in place | |
| | Offer this out to the schools to use for their MDM for iPads etc | Set requirements for MDM | |

| | | | |
|---|---|---|---|
| **Classroom Hardware** | Audit current hardware (screens etc) | Rolling replacement program<br><br>Investigate standardisation of classroom hardware to simplify training and shared learning | All classrooms in all schools have a minimum requirement (such as interactive screen) so that lessons can be engaging and fun and staff can move about more easily. |
| **Cloud Services/Platforms** | The trust isn't looking to restrict which platforms are subscribed to by the schools. Understand that different schools prefer different packages and have different needs. Looking to create an IT System that will support as many of these as possible. | Insist that wherever possible, all new systems have Single Sign on with a system that the school use (usually Office 365). This is for security and the ensure ease of use for pupils and staff | |
| **Printing** | Investigate current school contracts, Investigate Central Printing Solution | Schools contracts are expiring all schools join central system in place | |

# Annex

## Annex 1 – Security Standards

The below list of security standards for Microsoft 365 are indicative settings to be implemented.  More investigation will need to be undertaken to fully define the standards.

### Exchange

- Ensure Standard Protection is enabled
- Block malicious attachments
- Enable DKIM
- Enable DMARC
- Enable SPF
- Mailtips for external senders
- External email warning banner

### Entra

- Defender Alert policy set to forward to ICT Support
- Don't allow user consent for applications
- Users can create security groups disabled
- Users can register applications disabled
- P2 License purchased

### SharePoint

- Block apps that don't use Modern Auth
- Set Content sharing to new and existing guests
- Guest access expires after 30 days
- Default Link - Specific People
- Default Link - View Only
- Guests must sign in using the same account
- Don't allow guests to share items they don't own

### Conditional Access

- MFA For Admins Enforced
- MFA User Enforced - Staff
- MFA For Remote Users
- Lock Access Location
- User Risk Policy
- Sign in Risk Policy
- Block Legacy Authentication

### Windows Domain

- Limit Admin Accounts
- Configure Windows Firewall profile for all devices
- Security Defaults
- SRP or AppLocker, see WDAC for Intune
- Require that OS drives are encrypted
- Set up desktop admin user
- Lockout user after 10 incorrect attempts
- Lockout until admin unlocks
- Disable computer accounts older than 6 months
- Password policy, in line with NCSC
- Remote Users - Passwords expiry – 42 Days
- Ensure no services are running as domain admin

### Intune

- Set BitLocker policy
- Set up LAPS for cloud only devices
- Set ASR rules

### Microsoft 365 Settings

- Idle Session Timeout - 1 hour

### Microsoft Security

- Enable Defender for Endpoint
- Connect Defender to Intune
- Enterprise Apps - User consent - Set to do not allow

## Annex 2 – Backup Standards

We have chosen to use the DFE's Cloud solution standards for schools and colleges to provide our backups baseline.

Meeting digital and technology standards in schools and colleges - Cloud solution standards for schools and colleges - Guidance - GOV.UK

### Making sure that appropriate data backup provision is in place

DDAT will ensure that each schools data:

- Ensure what data is backed up
- Ensure where data is held (for UK GDPR compliance)
- How long is the data held for
- How frequently are backups made

To meet this standard, we should identify the data backup provision needed for each solution. This should be based on the data stored.

Consider:

- Data sensitivity
- Data importance to normal operations
- The impact if the data was to be unavailable temporarily or permanently
- How long the school or users could be without the data before it becomes an issue
- Balancing cost against need of the data; frequent backups are more expensive so consider the cost against the age of the data that needs recovering from a backup
- For critical data use the 3-2-1 rule, at least 3 copies, on 2 devices and 1 offsite

## Annex 3 – Networking Standards

It has been chosen to use the DFE's Network switching standards for schools and colleges and Wireless network standards for schools and colleges to provide our baseline.

Meeting digital and technology standards in schools and colleges - Network switching standards for schools and colleges - Guidance - GOV.UK

Meeting digital and technology standards in schools and colleges - Wireless network standards for schools and colleges - Guidance - GOV.UK

### Network switching standards

- Switches provide a minimum of 1Gbps connectivity to the user device
- Switches higher-speed (multi-gigabit) ports support devices and infrastructure equipment that needs high bandwidth
- Switches that connect to wireless access points, CCTV and telephones must comply with the correct PoE requirements outlined by the device manufacturer
- Where switches are stacked, they should support 40Gbps interconnects between switches in a stack, dedicated stacking ports should be used to enable high-speed communication between each switch in the stack
- Connections linking switches or switch stacks in hub rooms must connect back to the core server room using a minimum of 2x10Gbps with links taking different routes where possible. See dependencies on this standard.
- Switches providing POE should adhere to IEEE 802.3af.at or bt as required by the connecting device and have LLDP-Med enabled.
- Switches should:
    - have a minimum of 512MB of core memory
    - support a minimum of 16000 MAC addresses
    - support spanning tree protocols such as MST or RST
    - use non-blocking switch fabric
    - Switches should be Energy Efficient Ethernet compliant to a minimum of 802.3az standard or equivalent.
    - Provide a central management tool that can be used to configure the switching (core and edge), monitor performance and provide alerts in the event of a failure
    - Switches should include a manufacturer warranty and support arrangement (telephone, email and web) including licences, software enhancements and firmware updates, providing 5 years of cover as a minimum.
    - Include a system administrator training package on your school or college site that is:
        - approved by your manufacturer
        - appropriate to the scale of the solution
        - covering all security elements for the solution

- Ensure that switches are configured to support network segregation, security and quality of service. This should not impact the network's deployment or performance and should be aligned with the environment
- Any administrative accounts that have access to make configuration changes, must be secure and fully documented
- The delivery of software updates should be set to automatically update as soon as they are available and manual checks should also be undertaken
- Ensure that NACs and policy management implemented to ensure that authorised mobile user devices or guest user roles are securely authenticated onto the network. Network traffic should be protected from external and unauthorised internal interception
- Critical core switches should have at least:
    - 2 power supplies
    - 2 management modules
    - 2 connections to other critical infrastructure such as routers, servers and other core switches
- The critical core switches should be connected to at least 1 UPS

### Wireless network standards

- The wireless network should use the latest standard approved by the Wi-Fi Alliance, Wi-Fi 6 (802.11ax)
- The network interface speeds of the access points need to be considered, these will typically be 1Gbps, 2.5Gbps and 5Gbps
- The wireless network should be configured to support network segregation and QoS
- Investigate if needed:
    - virtual local area networks (VLANs)
    - access control lists (ACLs)
    - secure segregated guest access
    - the latest authentication protocols (WPA3)
    - wireless intrusion protection (WIPs)
    - certificate-based authentication
    - multi-factor authentication (MFA) for privileged users and technical support staff
- When procuring a solution:
    - Ensure that the number of access points provides coverage in each space that is in line with the planned occupation level. This is to support simultaneous use without reducing the performance.
    - Ensure that your wireless provider designs a solution that fully meets your needs. This should include using wireless heat mapping as part of initial planning and ensuring that impact from building management systems and other networks is minimised

- Provide active signal management and load balancing of user or device connectivity
- Have tools that can be used to configure the wireless access points, monitor performance and provide alerts in the event of a failure
- Include a manufacturer warranty and support arrangements including licences, software enhancements and firmware updates
- Include an on-site, system administrator training package, that is manufacturer approved and that covers all security elements for the solution
- Be scalable and can accommodate future higher bandwidth requirements
- Be capable of providing a configuration file that allows the solution to be reset to the original configuration for the school

## Annex 4 – Recommended Device Specification Examples

### Computer

- Windows Pro Licence
- 23” Monitor or greater
- HDMI
- Ideally USB C and USB A ports
- Intel i3 13th Generation Quad Core or greater
- 16GB Ram
- Lan Gigabit or greater
- Wi-Fi 6

### Laptop

- Windows Pro Licence
- 15” Screen or Greater
- HDMI
- Ideally USB C and USB A ports
- Intel i3 13th Generation Quad Core or greater
- 16GB Ram
- Wi-Fi 6

### Tablet

- Apple iPad
- 128GB or greater
- Wi-fi only model
- Standard iPad for Students
- Air or Pro for Staff
- Software and Security support for 5 years